# VERKONVALVONTAPALVELUN TOTEUTUS

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2011
Antti Laaksonen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

LAAKSONEN, ANTTI: Verkonvalvontapalvelun toteutus

Tietoliikennetekniikan opinnäytetyö, 37 sivua, 4 liitesivua

Syksy 2011

TIIVISTELMÄ

---

IT-ala on aikaavievimpiä aloja. Samalla kun pitäisi rakentaa uutta, kehittää palveluita ja opetella jo huomisen uusia järjestelmiä, ovat alan ammattilaisen päivät kuitenkin vanhojen asioiden toiminnan ylläpitämistä ja korjaamista. Tietoliikennelaitteiden ja verkkojen ongelmiin on kuitenkin ratkaisu, verkonvalvonta. Sillä voidaan selvittää ongelmat yleensä jo ennen niiden ilmeentymistä ja korjata mahdolliset pullonkaulat ennen kuin todelliset ongelmat alkavat.

Tämän opinnäytetyön tavoitteena on suunnitella vapaan lähdekoodin verkonvalvontajärjestelmä LahtiNetwork Oy:lle ja tuotteistaa järjestelmä palveluksi. Verkonvalvonta on osa verkonhallintaa, joka sisältää viisi yleistä osa-aluetta: vikatilanteiden hallinta, määrittelyjen hallinta, suorituskyvyn hallinta, käytön ja laskutuksen hallinta sekä turvallisuuden hallinta. Työssä määritellään SNMP-protokollaperheen tärkeimmät osat sekä SNMP:n toiminta eri OSI-mallin kerroksilla. Verkonvalvontajärjestelmät ovat yleisesti ottaen hyvin kalliitta. Avoimella lähdekoodilla olevia järjestelmiä on nykypäivänä jo hyvinkin paljon ja niistä löytyy jo pitkälti samat ominaisuudet kuin maksullisista. Kuitenkin maksullisten järjestelmien etuna on niiden erittäin helppo käytettävyys ja loppuun asti hiottu ja tyylikäs käyttöliittymä.

Cacti ja Zabbix ovat avoimen lähdekoodin verkonvalvontajärjestelmiä. Cactista puuttuu oleellinen Auto Discovery -toiminto ja laitteiden seuranta-agentit. Zabbix on kaikille ilmainen avoimen lähdekoodin verkonvalvontajärjestelmä, joka sisältää käytännössä kaikki samat ominaisuudet kuin maksulliset. Zabbix-järjestelmä sisältää täyden kontrollin webbikäyttöliittymän ja tiedot ovat tallennettuna käyttäjän valitsemaan tietokantaan, tunnetuimpana MySQL-tietokanta. Orion on maksullinen järjestelmä, jossa kaikki toiminnot ovat yksinkertaisia ja käyttöönotto nopeaa.

Mikäli verkonvalvonnan haluaisi tuotteistaa, olisi järkevää valita ilmainen Zabbix pienikokoiselle valvonnalle. Suuremmalle verkkokokonaisuudelle olisi suositeltavaa ottaa maksullinen ja käyttäjätuen sisältävä Orion-järjestelmä, koska mitä suuremmaksi verkko kehittyy, sitä enemmän kasvaa verkonhallinnan työmäärä. Verkonvalvonnalla voidaan myös saavuttaa suuria energiasäästöjä, mikä on askel parempaan tulevaisuuteen.

Avainsanat: verkonvalvonta, verkonhallinta, SNMP, MIB, Zabbix

Lahti University of Applied Sciences
Degree Programme in information Technology

LAAKSONEN, ANTTI: Implementation of a network monitoring system

Bachelor's Thesis in Telecommunications, 37 pages, 4 appendices

Autumn 2011

ABSTRACT

---

The IT industry is one of the most time consuming areas to work. At the same time when we should be building new systems and learning how to develop services for tomorrow's new systems, the days of the professionals are still spent in maintaining and fixing old systems. However there is a solution for the network and telecommunication equipment problems: network monitoring. It can find problems usually before they appear and fix potential bottlenecks.

The aim of this thesis was to design an open-source network monitoring system for LahtiNetwork Ltd. and to commercialize the system into a service. Network monitoring is part of network management, which includes five general areas: fault management, configuration management, performance management, accounting management, and security management. This thesis also defines the most important parts of the SNMP protocol family and how SNMP works on the levels of the OSI model. Network monitoring systems are generally very expensive. There are already quite a lot of Open Source systems available today and they have all the same properties as the commercial ones. However, the ones that cost money have the advantage of easy availability and high-end polished and elegant user interface.

Cacti and Zabbix are Open Source network monitoring systems. Cacti is missing the essential Auto Discovery feature and equipment monitoring agents. Zabbix is free for all and includes virtually all the same features as the commercial systems. Zabbix provides full control over the web browser and the monitoring data is stored to a selected database, the best known of which is the MySQL database. Orion is a premium commercial system. All of Orion's functions are simple and deployment is quick.

If you would like to commercialize network monitoring, it would make sense to choose a free Zabbix for a small supervised zone. For larger network it would be advisable to choose a commercial system, like Orion, which includes user support. The larger a network becomes, the more work there is for network management. Network Monitoring can also achieve large energy savings, which is a step towards a better future.

Key words: Network Monitoring, Network Management, SNMP, MIB, Zabbix

SISÄLLYS

LYHENNELUETTELO

| | |
|---|---|
| AES | Advanced Encryption Standard, lohkosalausmenetelmä. |
| ASN.1 | Abstract Syntax Notation One, merkintätapastandardi. |
| DES | Data Encryption Standard, symmetrinen lohkosalausmenetelmä. |
| GPL | General Public License, vapaan lähdekoodin julkaisemiseen tarkoitettu lisenssi. |
| IDS | Intrusion detection system, tunkeilijan havaitsemisjärjestelmä. |
| IETF | Internet Engineering Task Force, internetprotokollien standardoinnista vastaava organisaatio. |
| ITU-T | International Telecommunication Union – Telecommunnication, kansainvälinen televiestintäliitto. |
| IP | Internet Protoocol, internetprotokolla. |
| ISO | International Organization for Standardization, kansainvälinen standardisoimisjärjestö. |
| MAC | Media Access Control, fyysinen verkko-osoite. |
| MD5 | Message-Digest Algorithm, viestitiivistealgoritmi. |
| MIB | Management Information Base, SNMP-protokollanryhmän hallintotietokanta. |
| OID | Object Identifier, yksilöintitunnus MIB-hallintatietokannassa. |

| | |
|---|---|
| OSI | Open Systems Interconnection, (OSI-malli) määrittelee tietoliikennejärjestelmän kerrosrakenteisen verkkorakenteen. |
| RFC | Requests for Comments, IETF-organisaation julkaisemia standardeja. |
| RMON | Remote network Monitoring, SNMP:n laajennus, määrittelee hallintatietokannan verkkojen etähallintaan. |
| SLA | Service-level agreement, on asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot. |
| SMI | Structure of Management Information, määrittelee MIB-hallintatietokannan tietorakenteen. |
| SNMP | Simpe Network Management Protocol, TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla. |
| TCP | Transmission Control Protocol. |
| UDP | User Datagram Protocol, tiedonsiirron hallintaprotokolla. |
| VPN | Virtual Private Network, virtuaalinen salattu verkko. |
| WAN | Wide Area Network, laajaverkko, joka yhdistää lähiverkot. |

# 1 JOHDANTO

Opinnäytetyön tavoitteena oli kehittää LahtiNetwork Oy:lle verkonvalvontajärjestelmä, joka tulisi yhtiön tulevaan omaan konesaliin. Tavoitteena oli selvittää mahdollisimman monipuolinen, edullinen, dokumentoitu ja helppokäyttöinen järjestelmä, joka voitaisiin myöhemmässä vaiheessa jopa tuotteistaa palveluksi osaksi yrityksille tarjottaviin internetliittymiin. Yrityksessä sattuneista muutoksista johtuen, palvelinsalihanke viivästyi puolella vuodella ja verkonvalvontajärjestelmää ei päästy opinnäytetyön työstämisen aikana testaamaan lopullisessa ympäristössään. Tästä syystä konesalin tilalle rakennettiin pienimuotoinen laboratoria, joka pyrki simuloimaan tilannetta, missä verkonvalvontajärjestelmä valvoo useita eri aktiivilaitteita ja palvelimia sekä ilmoittaa hälytyksin järjestelmän vioista järjestelmänvalvojalle.

Tutkimusongelma työssä muodostui LahtiNetwork Oy:n pyynnöstä selvittää, onko mahdollista rakentaa järjestelmä erittäin rajatuilla resursseilla ja mahdollisesti jopa tuotteistaa palveluksi. Toiseksi vaatimukseksi järjestelmälle annettiin kasvun huomioiminen valvottavien laitteiden määrässä. Kolmas vaatimus järjestelmälle oli mahdollisimman yksinkertainen ja helppo käyttöliittymä, josta voidaan tehdä kaikki tarpeelliset muutokset. Neljäntenä oli yrityksen nuoresta iästä johtunut taloudellinen tilanne, jonka vuoksi järjestelmän piti olla avoimella lähdekoodilla toteutettu. Viides vaatimus oli tehdä asennusohje järjestelmälle.

Opinnäytetyössä käydään läpi verkonvalvonnan eli hallinnan keskeisimmät asiat ja tietoliikenneprotollat, joiden tuntemus järjestelmän ylläpidossa on välttämätöntä. Verkonvalvontasovelluksen valinta työssä on tehty vertailun kautta. Vertailukriteerit olivat isossa roolissa, joten valintaan oli otettava vain kaksi varsinaisesti vapaan lähdekoodin sovellusta, Zabbix ja Cacti. Tämä siksi, koska sovelluksissa oli riittävän kattava ja tarpeeksi yksinkertainen käyttöliittymä. Lisäksi ajatellen yhtiön tulevaisuuden laajenemissuunitelmia, oli vertailuun otettava vielä yksi maksullinen sovellus, Orion.

Verkonvalvonnan tuotteistaminen oli yksi yrityksen toiveista, joten työssä on pohdittu, miten verkonvalvonta voitaisiin tuotteistaa. Samalla on luotu tuotekuvaus ja pohdittu tuotteen yksikköhinnoittelua. Vaatimus oli myös saada projektista dokumentaatio (opinnäytetyö), jonka perusteella voitaisiin verkonhallintajärjestelmä asentaa ja ottaa käyttöön uudestaan nopeasti uudelle ajanmukaisemmalle kokoonpanolle, kun sitä tarvittaisiin. Työssä on myös pohdittu hypoteettisesti, kuinka verkonvalvontajärjestelmä voitaisiin myös toteuttaa keskitetysti etänä yritysasiakkaiden verkkoihin.

Tutkimuksessani käytetty aineisto pohjautuu pitkälti internetissä oleviin protokollien stadardoituihin webbiaineistoihin, vapaaseen tietosanakirjaan (Wikipedia) sekä julkastuihin kirjallisuusteoksiin. Johtuen alan huiman kehityksen vuoksi, on tietolähteeksi valittu useimmiten webbilähde.

# 2 VERKONHALLINTA JA VALVONTA

## 2.1 Verkonhallinta

Internetin käyttö, lähiverkkojen koko ja käyttö ovat räjähdysmäisesti kasvaneet viimeisinä vuosikymmeninä. Infrastruktuurin kasvaessa tarvitsevat yritykset ratkaisuja verkon toimivuuden ylläpitämiseksi. Lähes kaikki yritykset ovat tänä päivänä riippuvaisia toimivasta lähiverkosta ja internetistä, jossa pienikin katkos saattaa pysäyttää suuren yrityksen toiminnan kokonaan, koska yhä enemmän ja enemmän palveluita siirretään palvelimille ja pilveen. Katkokset saattavat aiheuttaa hyvinkin mittavia tappioita yritykselle kuin yritykselle toimimattoman verkon takia. Tarve valvoa verkkoa on kasvava, koska riippuvuus verkon toimivuudesta on elintärkeä. (Puska 2000, 306.)

Verkonhallinta sisältää viisi yleistä osa-aluetta: vikatilanteiden hallinta, määrittelyjen hallinta, suorituskyvyn hallinta, käytön ja laskutuksen hallinta sekä turvallisuuden hallinta. Osa-alueet on määritelty ITU-T (International Telecommunication Union – Telecommunnication) verkonhallintastandardissa X.700. Standardi kattaa kaikki verkkotekniikat, mutta painottuu lähiverkkotekniikkaan, lähinnä vian-, suorituskyvyn ja määrittelyjen hallintaan. (Puska 2000, 306 - 307.)

Vikatilanteiden hallinta (Fault Management) parantaa verkon luotettavuutta antamalla verkon ylläpitäjälle työkalut tiedostamaan verkon tilan, kriittisien tapahtumien tallentamisen sekä vikojen nopean rakaisemisen. Vikalokeja voidaan hyödyntää myöhemmin vastaavissa vioissa sekä suunnittella vikasietoisempia verkkoja. Vikalokeja voidaan myös käyttää, kun on selvitettävä uusien laitteiden tarve. (Puska 2000, 306.)

Määrittelyjen hallinta (Configuration Management) sisältää tiedon verkon laitteista ja resursseista sekä niiden välisistä yhteyksistä. Määrityksiä voidaan käyttää hyväksi vianhaussa ja eristyksessä sekä verkon suunnittelussa. (Puska 2000, 306.)

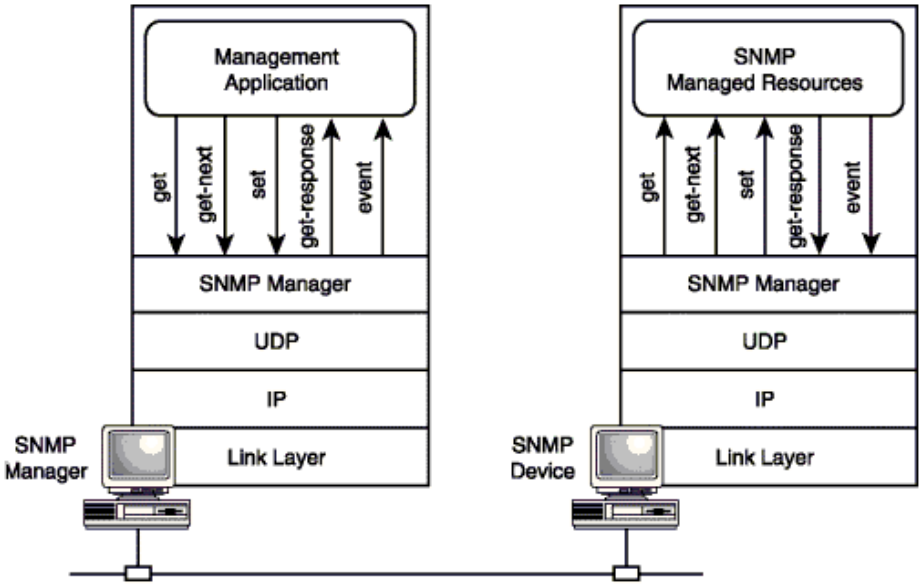
Suorituskyvyn hallinta (Performance Management) kuvaa parhaiten juuri toimintoaan, eli sillä pyritään ylläpitämään verkon suorituskykyä riittävän korkealla tasolla. Yleisin mittari on tehdä ping-testi, josta selviää vasteaika kyselyvastaukselle ja mahdollisesti voidaan korjata verkon pullonkaulat. Verkon kapasiteettia ja verkon kuormitusastetta käytetään myös hyvin paljon, johtuen osittain mittaamisen helppoudesta. (Puska 2000, 306–307.)

Käytön ja laskutuksen hallinta (Accounting Management) seuraa ja mittaa käyttäjien liikennettä sekä resurssien todellista käyttöä verkossa. Saaduilla tiedoilla voidaan rajoittaa käyttäjien liikennettä halutulla tavalla sekä laskuttaa esimerkiksi vuokraverkon kuormituksesta siirretyn tiedon määrän perusteella. (Puska 2000, 307.)

Turvallisuuden hallinta (Security Management) on pitkälti kontrolloitua käyttöoikeuksien jakoa niille, joille lukuoikeudet haluttuun tietoturvatasoon liittyen ovat aiheellisia. Tärkeä osa on myös verkkoon ja siihen liitettyjen laitteiden pääsyn seurantaa ja kontrollointia, lokien keräämistä, tallennusta ja sekä analysointia että mahdollisia tietomurtohälytyksiä. (Puska 2000, 307.)

## 2.2 SNMP

SNMP (Simple Network Management Protocol) on tietoliikenneprotokolla, jota käytetään TCP/IP (Transmission Control Protocol / Internet Protocol) -verkkojen hallinnassa. Protokolla mahdollistaa verkossa olevien aktiivilaitteiden ja päätelaitteiden hallinnan ja valvonnan yksinkertaisilla kyselyillä ja käskyillä (kuvio 1). SNMP-protokollan kehitti IETF (Internet Engineering Task Force), protokolla koostuu useista RFC-dokumentista (Requests for Comments), jotka kuvaavat itse SNMP:n, MIB:n (Management Information Base) eli hallintatietokantojen määrittelyn sekä SMI:n (Structure of Management Information) eli joukon tieto-olioita. (SNMP Research International inc. 2011.)




KUVIO 1. SNMP-arkkitehtuuri (Microsoft TechNet 2011)

Yleisesti ottaen SNMP:tä käytetään verkonvalvontajärjestelmissä ja ylläpidon tietokoneissa vastaanottamaan verkossa toimivilta aktiivilaitteilta ja päätelaitteilta tilapäivitysmuutoksia. Jokaisessa valvottavassa SNMP-laitteessa on agentti, johon on ennalta määritelty tilapäivitysmuutoksia vastaanottavan laitteen osoitetiedot. Vastaanottava laite toimii managerina, laite voi myös lähettäää käskyjä agentille, joka voi suorittaa käskyt laitteessa. (Wikipedia 2011a.)

Protokollasta on olemassa kolme erilaista versiota: SNMPv1, SNMPv2 ja SNMPv3. Versio kolme on IETF:n suosittelema standardi, muut ovat osa historiaa, mutta silti vieläkin vahvasti käytössä. SNMPv1 muodostui standardiksi vuonna 1990 ja kärsii puuttellisesta tietoturvasta, lähinnä sen yksinkertaisuuden ja salaamattoman liikenteen takia. SNMPv2:n ero ensimmäiseen versioon on turvallisuuden parantuminen. Siinä on mahdollista autentikointi. Tiedon salaus tapahtuu DES-algoritmilla ja tiedon eheys on varmistettavissa MD5-algoritmilla (Message Digest algorithm 5). SNMPv3:n suurin etu on sen parannettu salattu liikenne; salauksina voidaan käyttää kolminkertaista DES-salausta (Data Encryption Standard) tai jopa 256-bittistä AES-salausta (Advanced Encryption Standard). (Wikipedia 2011a.)

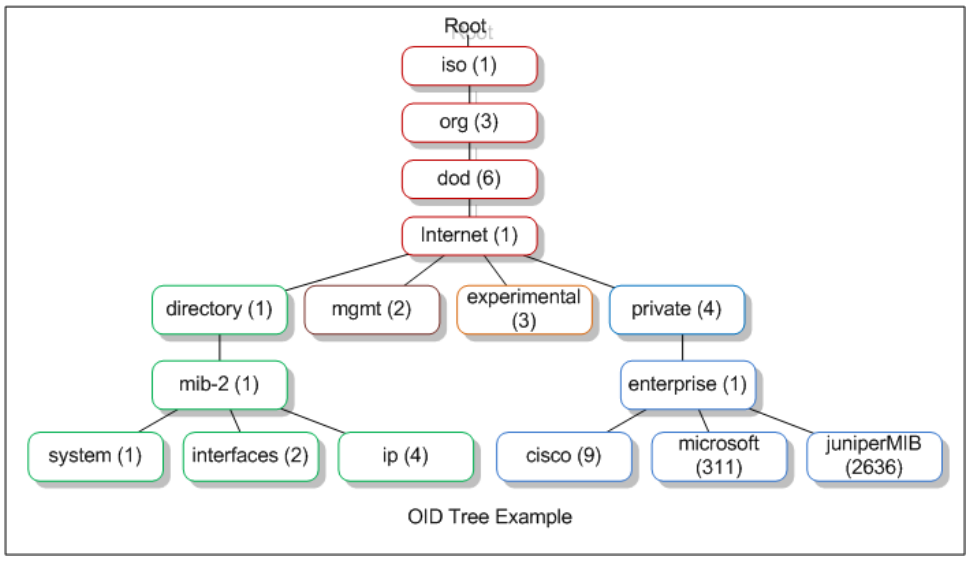
SNMP-agentti käyttää UDP-porttia 161 viestien vastaanottamiseen ja SNMP-manager niin ikään viestien lähettämiseen. SNMP-manager taas käyttää porttia 162 viestien vastaanottamiseen agentilta. Manager viestittää kuudella erilaisella viestillä agentille. Trap-viestit taas ovat ainoita viestejä, joita agentit eli valvottavat laitteet voivat generoida ja lähettää managerille. Viestityyppejä laitteiden väliseen kommunikoimiseen on seitsemän erilaista:

- GetRequest – pyydetään tietyn objektin arvo
- GetNextRequest – pyydetään seuraavan objektin arvo
- SetRequest – asetetaan tietyn objektin arvo
- GetResponse – vastaus Get tai Set pyyntöviestiin
- Trap – raja-arvon ylitysviesti
- InformRequest – vastaus Trap-viestiin
- GetBulkRequest – Optimoitu GetNextRequest.

(Wikipedia 2011a.)

## 2.3 MIB, SMI ja OID

MIB (Management Information Base) on hallintatietokanta, joka sisältää valvottavan laitteen tai verkon tiedot numerotunnisteena SMI:n määrittelemässä puumaisessa rakenteessa. ISO (International Standard Organization) määrittelee MIB-puun yläosan objektit (kuvio 2), kun taas puun alaosan määrittelee laitetoimittajat ja eri organisaatiot. Jokainen tietokannan objekti mittaa jotain tiettyä arvoa laitteesta tai verkosta. Muuttuneet tiedot välitetään SNMP-managerille, joka tulkitsee tiedon laadun. MIB-tietokannasta on olemassa kaksi eri versiota, MIB I ja laajempi MIB II. (Wikipedia 2011b.)




KUVIO 2. SNMP MIB OID -puurakenne-esimerkki (Network Management Software 2011)

SMI (Structure of Management Information) määrittelee säännöt ja MIB:n hallintatietokantojen määrittämiselle ja luomiselle ASN.1-standarin (Abstract Syntax Notation One) mukaan. SMI:stä on olemassa kaksi versiota. Ensimmäisen version määrittelee RFC1155 ja toisen RFC2578. SMI:n määrittely on jaettu kolmeen osaan: moduulien-, objektien- ja ilmoitusten määrittely. (RFC2578 1999, 2-3.)

OID (Object Identifier) on hallintotietokannan (MIB) objekti, joka voidaan tunnistaa ASN.1-standardin määrityksillä. Jokaiselle tietokannan objektille on annettu tunnistenumero eli OID. Esimerkkinä (kuvio 2) 1.3.6.1 -alkuinen numero, joka voidaan esittää myös muodossa iso.org.dod.internet. OID:t ovat kuin MIB:n puhelinluettelo. (RFC1213 1991, 9.)

Jokaisella objektilla on nimi, syntaksi ja koodaus. Nimi on OID:n tyyppiä/toimintaa kuvaava tieto, joka selittää itsessään, mihin objekti viittaa. Syntaksi kuvaa kyseisen objektin sisältämän abstraktin tietorakenteen, mihin kyseinen data viittaa. Koodaus määrittelee yksinkertaisesti objektin tyypin ja tyypin muodon, kuinka juuri kyseinen objekti on uudelleen luettavissa objektityypin syntaksilla. Yksinkertaistettuna, objektin tyypin syntaksi ja koodaus määrittelevät objektin ulkoasun ennen verkkoon lähettämistä. SMI määrittelee ASN.1:n peruskoodauksen säännöt, joita SNMP:n asettamat lisävaatimukset vaativat. (RFC1213 1991, 9.)

## 2.4 RMON

RMON (Remote Network Monitoring) luotiin vähentämään SNMP:n aiheuttamaa verkkoliikennettä. SNMP ilmoittaa ilmoittaa valvottavastaan laitteesta managerille aina, kun raja-arvo ylittyy. Tämän seurauksena verkkoon on mahdollista syntyä pullonkauloja. Syy, miksi RMON kehitettiin, oli muuttaa valvontaa siten, että valvottavat laitteet lähettävät ensin verkkosegmentistään tietoa yhdelle RMON-agentille, joka säilyttää ja kokoaa tiedot laitteista ja lähettää tiedot hallitusti ja keskitetysti RMON-managerille, verkonvalvojalle. Toinen syy on varmistaa tiedon kulku managerille, koska SNMP-pohjaisessa liikenteessä ongelmaksi koituisi UDP-liikenne. Ongelma lähinnä voisi syntyä, kun SNMP-agentit joutuisivat lähettämään tietoa esimerkiksi yrityksen sivutoimipisteestä toiselta mantereelta toiselle, esimerkiksi pääkonttorille, koska tärkeä data ei välttämättä pääsisi perille asti tiedon UDP-pohjaisuudesta johtuen. (Wikipedia 2011c.)


KUVIO 3. OSI-malli (Wikipedia 2011d)

Alkuperäinen RMON1-versio keskittyy lähinnä OSI-mallissa (kuvio 3) 1. fyysiselle- ja 2. siirtoyhteyskerrokselle. Toinen versio, RMON2 on lähinnä laajennusversio ensimmäiseen. Lisäyksenä on tullut laajennus OSI-mallin 3. verkko- ja 4. kuljetuskerros. SMON (Switch Monitoring) on niin ikään laajennus, joka tarjoaa piirikytkettyjen verkkon tuen. RMON-toiminnot toimivat palvelintyyppisesesti erillislaitteena tai ovat ominaisuutena operaattoritason aktiivilaitteissa. (RFC2613 1999, 2-3; Wikipedia 2011c.)

RMON1 MIB-tiedot sisältää kymmenen eri ryhmää:

1. Statistics – Verkon statistiikka
2. History – Ennalta määriteltyjen tietojan historia
3. Alarms – SNMP-raja-arvojen ylitykset
4. Hosts – Päätelaitteiden statistiikka
5. Hosts top N – Aktiivisten yhteyksien määrä ajanjaksolla N
6. Matrix – Eri järjestelmien välillä tapahtunut liikenne
7. Filter – Ennalta määritellyt paketit
8. Capture – Kaapattujen pakettien keräys ja uudelleen lähetys
9. Events – SNMP-trap-viestien lähetys
10. Token Ring – Laajennus verkon toimintojen määrittämiseksi (Wikipedia 2011c).

RMON2 laajennukset hallintatietoihin:

1. Protocol Directory – Lista monitoroitavista protokollista
2. Protocol Distribution – Verkkokerroksen protokollien liikennetilastot
3. Address Map – Verkkokerroksen osoitekartta
4. Network-Layer Hosts – Verkkokerroksen päätelaitteet
5. Network-Layer Matrix – Verkkokerroksen liikennetilastot eri järjestelmien välillä
6. Application-Layer Hosts – Ohjelmistokerroksen protokollien liikennetilastot päätaleitekohtaisesti
7. Application-Layer Matrix – Ohjelmistokerroksen protokollien liikennetilastot eri järjestelmien välillä
8. User history – Käyttäjähistoria
9. Probe Configuration – RMON-laitteiden etämäärittely
10. RMON Conformance – RMON2 MIB vaatimusten määrittely (Wikipedia 2011c).

## 2.5 OSI-malli

Tietoliikenteen yksi tärkeimmistä standardeista, joka kuvaa koko tiedon tapahtumia liikkuessa järjestelmästä toiseen, on ISO:n (International Organization for Standardization) määrittelemä OSI-viitemalli (The Open Systems Interconnection model) (kuvio 1). OSI-malli suunniteltiin aikoinaan yhtäläistämään eri laitevalmistajien väliset laite-erot siten, että kaikki laitteistot ja ohjelmistot voisivat keskustella toistensa kanssa täysin yhteensopivasti. Ajatuksena oli luoda avoin laitteisto- ja ohjelmistomaailma, jossa käyttäjän ei tarvitsisi miettiä, mitä asioita ostaa yhteensopimattomuuden pelossa. Kuitenkin kilpailu maailmalla voitti standardin eikä avoimia OSI-mallin mukaisia järjestelmiä tullut laajamittaisesti käyttöön. OSI-malli on kuitenkin tietoliikennejärjestelmien kuvaamisessa yksi yleisin käytetyimmistä metodeista mallin yksinkertaisuudesta johtuen. (Hakala & Vainio 2005, 138.)

OSI-mallissa on seitsemän kerrosta (kuvio 4), joista jokainen kerros kuvaa yhtä perustehtävää tietojärjestelmässä. Kolme alinta kerrosta määrittelevät verkkolaitteiden, median sekä niissä käytettyjen protokollien käytön. Neljä ylintä kerrosta määrittelevät päätelaitteiden välillä tapahtuvan liikenteen ja siinä käytetyt protokollat. (Hakala, M & Vainio, M 2005, 138.)


KUVIO 4. OSI-malli (Wikipedia 2011d)

Fyysinen kerros (Physical layer) (1. kerros) määrittelee median ja signaalinsiirtoon liittyvät mekaaniset ja sähköiset arvot. Kerros määrittelee kaapeleissa kaiken tarvittavan, kuten kaapelityypin, liittimet, vaimennukset, signaalin jännitetasot, heijastukset. Fyysinen kerros myös määrittelee mediakoodauksen signaalityypille, mille bitit muutetaan, kuten sähkökaapelille, valokuidulle tai radioaallolle. Kaapelin toimivuudet mitataan OSI-mallin mukaisin määrityksin. Aktiivilaitteista vain toistimet, keskittimet ja mediamuuntimet kuuluvat varsinaisesti fyysiselle kerrokselle. (Hakala, M & Vainio 2005, 139.)

Siirtoyhteyskerros (Data link layer) (2. kerros) määrittelee kaapelointijärjestelmään siirrettävän datan muodostamisen alimman tason kehykset, fyysiset MAC-osoitteet (Media Access Control). Kerroksen tärkeimmät aktiivilaitteet ovat päätelaitteiden verkkokortit ja kytkimet. (Hakala, M & Vainio 2005, 139.)

Verkkokerros (Network layer) (3. kerros) määrittelee reitit ykset ja niiden priorisoinnit verkkojen välisellä tietoliikenteellä. Loogiset IP-osoitteet määrittelee IP-protokolla (Internet Protocol), jonka avulla voidaan määritellä tiedon kulku oikeaan osoitteeseen verkoissa. Verkkokerroksen tärkein aktiivilaite on reititin. (Hakala, M & Vainio 2005, 139.)

Kuljetuskerros (Trasport layer) (4. kerros) määrittelee kuljetusprotokollien toiminnan. Tärkein tehtävä on ojelmien datan pilkkominen riitävän pieniin paketteihin ja varmistetaan, että paketit tulevat oikeassa järjestyksessä päätelaitteelle, yhteyden muodostuksen ja purkamisen sekä tiedon perille pääsyn varmistuksen. Vuonohjaus on myös kerroksen tehtävä. Toiminnoista vastaa nykyään lähes aina TCP-kuljetusprotkolla (Transmission Control Protocol). Samalla kerroksella toimii myös TCP/IP-protokollaperheen UDP-protokolla (User Datagram Protocol). UDP-protokolla taas ei varmista perille pääsyä, jonka vuoksi sitä kutsutaan yhteydettömäksi protokollaksi. (Hakala, M & Vainio 2005, 139 - 140.)

Yhteysjakso- eli istuntokerros (Session layer) (5. kerros) vastaa useiden eri ohjelmistojen yhtäaikaisen liikenteen multipleksoinnista, eli eri tietojen lähettämisestä samanaikaisesti samaan mediaan. Tämä on mahdollista, koska kaikki data pilkot-

tiin edellä mainitusti paketteihin, joissa jokaisessa on tiedot vastaanottavan osoitteesta. (Wikipedia 2011a.)

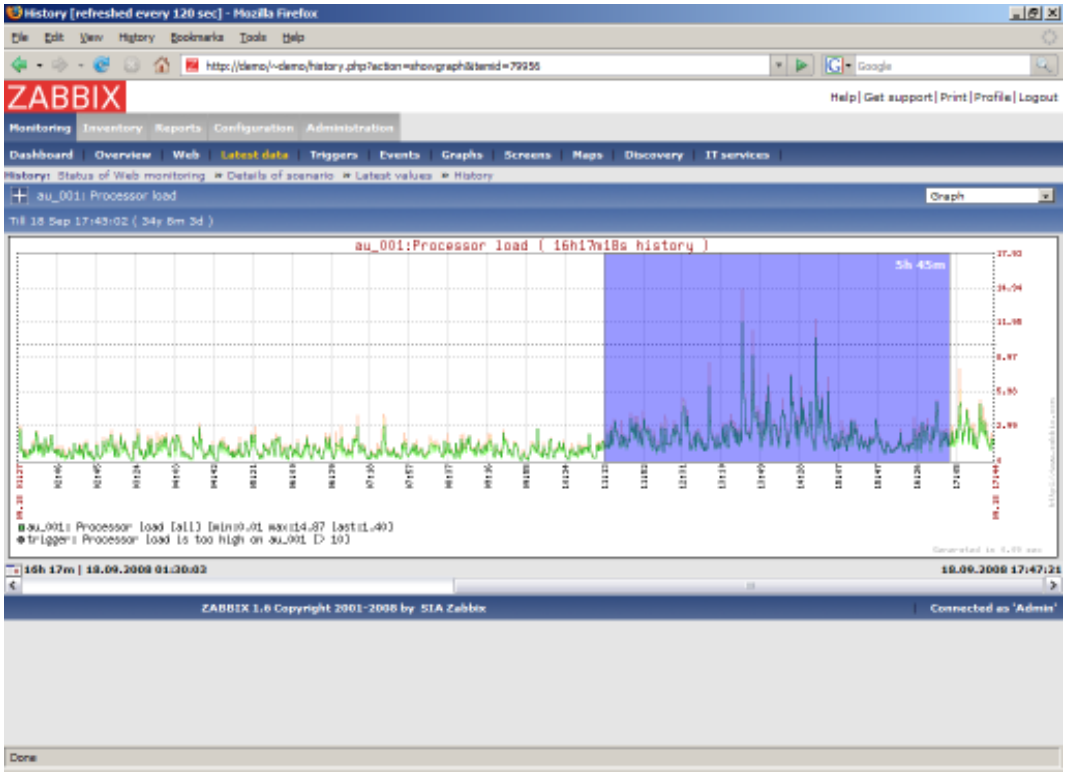
Esitystapakerros (Presentation layer) (6. kerros) määrittelee asiakkaan ja palvelimen välisen merkistökoodauksen yhteensovittamisesta oikeaksi tiedonsiirron yhteydessä. Kerroksen tehtävänä on päättää, missä muodossa esimerkiksi teksti, kuva tai ääni esitetään tiedonsiirron yhteydessä ja saada vastaanottava myös ymmärtämään tiedon muoto. (Hakala, M & Vainio 2005, 140.)

Sovelluskerros (Application layer) (7. kerros) määrittelee loput osat, joita aikaisemmissa kerroksissa ei ole määritelty. On kuitenkin hyvä huomioida, ettei OSI-malli ole tänä päivänä enää sama kuin ennen, vaan esimerkiksi sovellu-, esitystapa- ja istuntokerrokset muodostavat käytännössä yhden ison ohjelmallisen kokonaisuuden, josta ei yhtä ole mahdollista erottaa. Kuitenkin TCP/IP-protokolliin pohjautuvissa ohjelmistoissa voidaan esitystapakerros yleensä erottaa. (Hakala, M & Vainio 2005, 140–141.)

# 3 VERKONVALVONTASOVELLUKSET

## 3.1 Zabbix

Zabbixin on luonut Alexei Vladishev. Latvialainen Zabbix SIA kehittää aktiivisesti Zabbix-verkonvalvontaohjelmistoa. Järjestelmä on luokiteltu suuryritysluokille. Ohjelmisto valvoo lukuisia parametreja verkosta ja palvelimien palveluiden toimivuutta. Ohjelmistossa on myös joustava ilmoitusmenettely, jonka avulla käyttäjien on mahdollista määrittää ilmoituksia käytännössä aivan kaikista tapahtumista sähköpostitse. Vaihtoehtoisia ilmoituksia voidaan myös luoda tekstiviesteiksi, Jabber-viesteiksi tai äänihälytyksiksi. Näiden hälyksien avulla on mahdollista saada nopeat vasteajat ongelmien havaitsemiseksi ja korjaamiseksi. Zabbixin keräämä informaatio tallentuu tietokantaan, josta sitä on helppo lukea ja raportoida valmiilla visuaalisilla toiminnoilla tai ulkopuolisilla ohjelmistoilla. Tietokantojen ansiosta Zabbix on ideaalinen kapasiteetin sunnitteluun (kuvio 5). (Zabbix SIA 2011a.)




KUVIO 5. Zabbix – Prosessorin kuorma (Zabbix SIA 2011b)

Ohjelmisto tukee sekä kyselyn lähettämistä (Polling) että ilmoituksien lähettämistä (Trapping). Kaikki Zabbixin raportit, statistiikka ja määrittelyt ovat helposti saatavilla nettikäyttöliittymän kautta. Tämä mahdollistaa järjestelmän tarkkailun mistä tahansa maailmaa webbiselaimen kautta, mikä on nykypäivänä elintärkeää, kun järjestelmien ylläpidot monesti ulkoistetaan yrityksen ulkopuolelle. Zabbix sopii sekä pienille että suurille valvontaympäristöille. (Zabbix SIA 2011a.)

Zabbix on täysin ilmainen sekä koodattu että jaettu lisenssillä GPL 2 (General Public License version 2). Tämä tarkoittaa, että Zabbix-lähdekoodi on täysin vapaasti jaettavissa kaikille. (Zabbix SIA 2011a.)

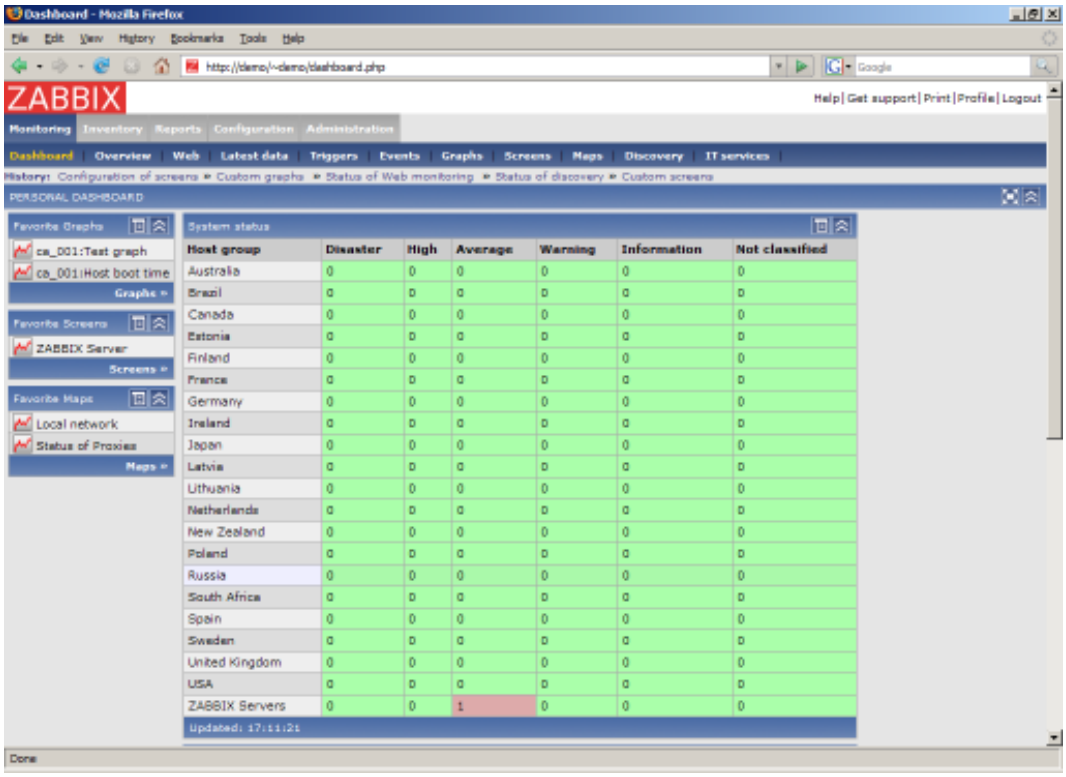
Zabbix tarjoaa seuraavat palvelut:

- Auto Discovery palvelimille sekä aktiivilaitteille
- yleinen seuranta sekä keskitetty järjestelmän WEB-hallinnointi
- tuki molemmille ilmoitus ja kyselymekanismeille
- tuetut käyttöjärjestelmät palvelimelle:
    - Linux
    - Solaris
    - HP-UX
    - AIX
    - FreeBSD
    - OpenBSD
    - OS X
- natiivit agentit seuraaville päätelaitteille:
    - Linux
    - Solaris
    - HP-UX
    - AIX
    - Free BSD
    - OS X
    - Tru64/OSF1
    - Windows NT 4.0, 2000, 2003, XP ja Vista
- agentiton seuranta

- turvallinen käyttäjätunnistus
- joustavat käyttäjäoikeudet
- web-pohjainen käyttöliittymä
- joustavat email-ilmoitusten lähetys ennalta määritellyistä tapahtumista
- korkeatasoinen verkonvalvonta näkymä
- logien tarkastelu (Zabbix SIA 2011a.)

Zabbixin käytön hyödyt pitkälti ovat lähinnä vapaa lähdekoodi, agentit UNIX ja WIN32-pohjaisille käyttöjärjestelmille. Zabbix on helppo omaksua, käyttää ja on yllättävän yksinkertainen kokoonpanoltaan. Ohjelmistossa on keskitetty seuranta-järjestelmä, joka sisältää kaikki tiedot kokoonpanosta, suorituskyvystä ja datasta tallennettuna relaatiotietokantaan. Zabbixin asennus on helppo, kun osaa seurata Zabbixin kotisivuilla olevaa ohjetta. Ohjelmistossa on tuki SNMP versiolle 1 ja 2 ilmoitus- ja kyselyviesteille. Ohjelmistossa on kattavat visualisointiominaisuudet kerätylle datalle sekä kattava sisäänrakennettu taloudenhoitomenettely tietomäärien ylläpitämiseen. (Zabbix SIA 2011a.)

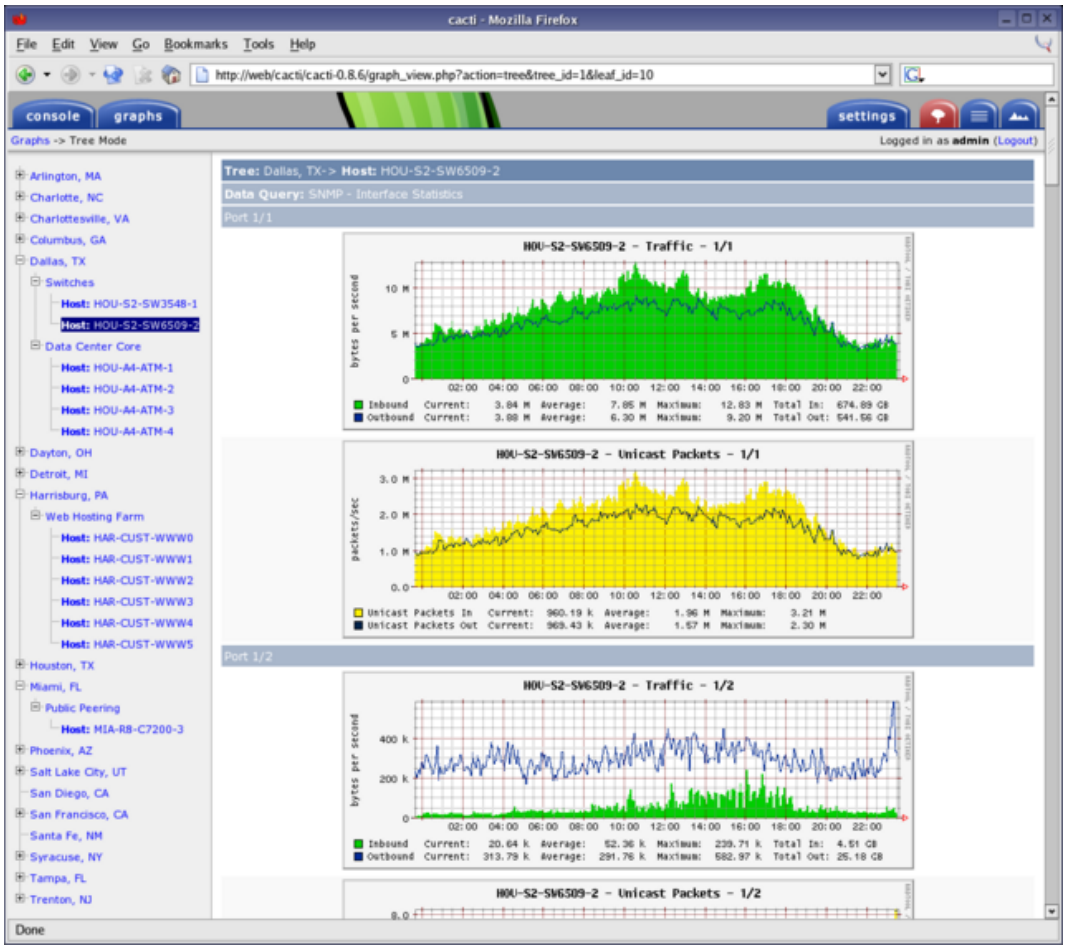
Zabbixin pääperiaatteita ovat käyttäjäystävällisyys ja asioiden pitäminen yksinkertaisina (kuvio 6). Tärkeää on ollut suunnitella järjestelmä, joka käyttää mahdollisimman vähän resursseja käsittelyyn. Ohjelmistossa on myös nopea reagointikyky huomautettaviin asioihin. Pääperjaatteena on myös kaikki ohjelmiston ominaisuuksien dokumentointi, koska kyseessä on vapaan lähdekoodin ohjelmisto. (Zabbix SIA 2011a.)




KUVIO 6. Zabbix – Yksinkertainen perusnäkymä (Zabbix SIA 2011b)

## 3.2 Cacti

Cacti on käytännössä vain käyttöliittymä, joka tulkitsee kerättyä dataa ja logitietoja MySQL-tietokannasta piirtäen niistä hienoja kuvaajia ja käppyröitä (kuvio 7) havainnoimaan muutoksia verkonvalvonnassa. Käyttöliittymä on täysin PHP-pohjaisesti ohjelmoitu toimimaan Internet-selaimessa. Cacti huolehtii myös kuvaajien ja tietojen lisäksi tiedon keruusta. SNMP-optiota voidaan myös käyttää luomaan liikennekuvaajia MRTG:lla (Multi Router Traffic Grapher). (The Cacti Group 2011a.)




KUVIO 7. Cacti – käyttöliittymä (The Cacti Group 2011b)

Hallitakseen tietolähteitä ja niiden datankeruuta tietokantaan on tietolähteet ensin määriteltävä joko ulkoisilla scripteillä tai sisäänrakennetuilla komenoilla. Tämän jälkeen Cacti luo määrityksistä cron-tapahtuman (ajastettu tapahtuma), joka toistaa itseään käyttäjän määrittelemällä tavalla ja tallentaa kerätyn datan tietokantaan. Esimerkiksi, jos käyttäjä haluaisi luoda ja määritellä kuvaajaksi ping-vasteajat, voi käyttäjä luoda scriptin, joka tekee yksinkertaisen ping-kyselyn ja palauttaa vasteajan arvon. Kun uusi tietolähde on määritelty, suorittaa ohjelma sen automaattisesti viiden minuutin välein, eli suorittaa ping-kyselyn ja palauttaa siitä vasteajan tietokantaan, josta Cacti ylläpitää kuvaajia. (The Cacti Group 2011a.)

Cactissa on mahdollista luoda eritasoisia luku- ja kirjoitusoikeuksia. Tämän ansiosta voidaan tietyille käyttäjille antaa mahdollisuus tehdä muutoksia kuvaajien parametreihin, kun taas osalle käyttäjille voidaan antaa vain lukuoikeudet tiettyi-

hin kuvaajiin. Jokainen käyttäjä myös hallitsee, miten kuvaajiaan haluaa tarkastella. (The Cacti Group 2011a.)

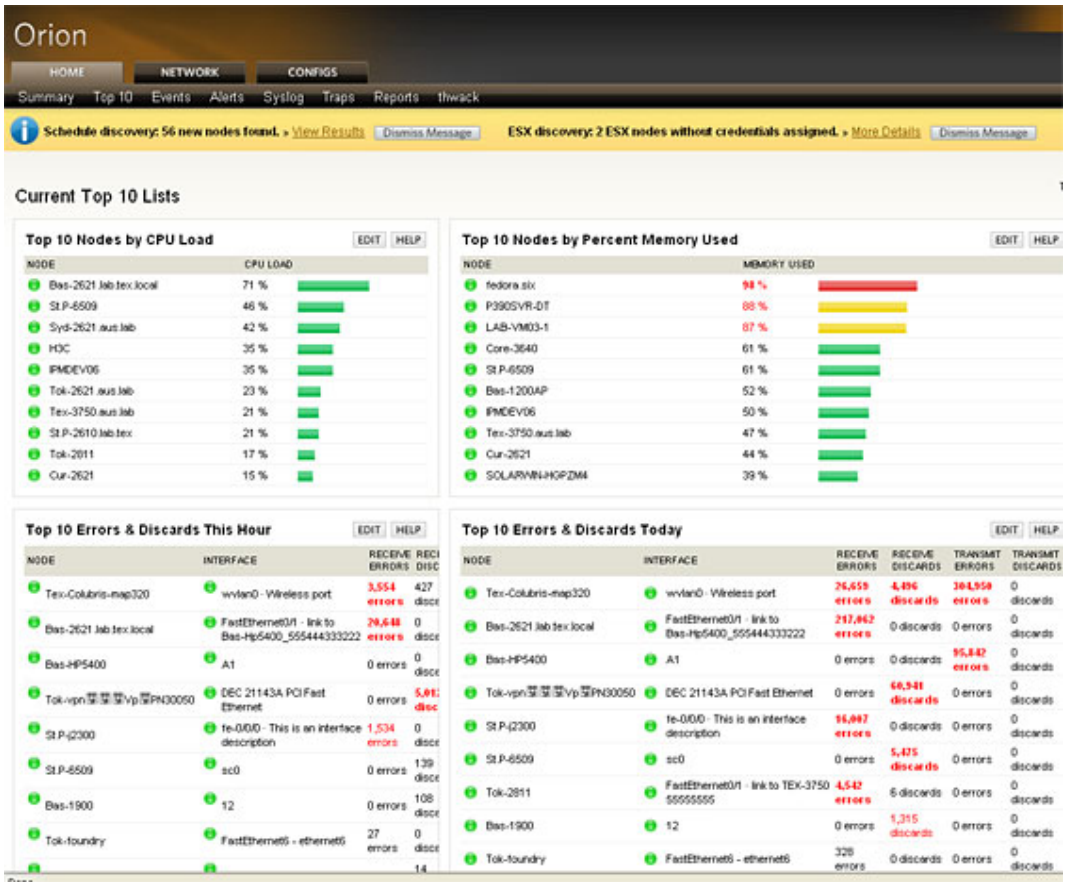
Mallipohjien luonti on mahdollista Cactissa. Niiden avulla voidaan ottaa samoja tiedonkeruumetodeja käyttöön helposti laajoissakin valvottavissa järjestelmissä ilman, että kaikki tietolähteet ja siihen liittyvät scriptit olisi määriteltävä uudestaan luotaessa uusia kuvaajia valvottavista asioista. (The Cacti Group 2011a.)

## 3.3 Orion

Orion Network Performance Monitor (NPM) antaa yksityiskohtaisia valvontatietoja ja analyysejä reitittimien, kytkimien, servereiden ja muiden SNMP-laitteiden suorituskyvystä. Orion selvittää automaattisesti verkon laitteet ja näyttää suorituskykystatistiikat reaaliajassa dynaamisen verkkotopologia karttana. Järjestelmä sistältää myös laatikon ulkopuolelta kaiken sisältämän aloitussivun, hälytykset ja raportit. (Solarwinds 2011a.)

Solarwinds Network Performance Monitor mahdollistaa nopean vian havaitsemisen, diagnosoimisen ja ratkaisemisen verkon suorityskykyongelmissa ja katkokset ennen kuin ylläpito alkaa saada puhelinsoittoja verkon alhaallaolosta. Orion on myös helpoin tuote ottaa käyttöön, käyttää ja ylläpitää. Tämän johdosta ylläpidon on mahdollista keskittyä hallinnoimaan verkkoa eikä verkonvalvontasovellusta. Järjestelmä on mahdollista ottaa käyttöön jopa tunnissa, toisin kuin muut esimerkiksi avoimen lähdekoodin järjestelmät, joita saattaa joutua määrittelemään jopa viikkoja. (Solarwinds 2011a.)

Orion on kattava verkon suorituskyvyn valvontasovellus myös moniosaisille verkoille. Järjestelmä valvoo, seuraa laitteiden ylhäälläoloa ja analysoi reaaliajassa verkon aktiivi- ja päätelaitteiden suorituskyvyn statistiikkaa (kuvio 8). Intuitiivinen käyttöliittymä toimii tarjoamalla tietoa laite laitteelta yksityiskohtaisia järjestelmätietoja verkkolaitteista, palvelimista ja virtuaalikoneista. (Solarwinds 2011a.)




KUVIO 8. Orion suorituskyvyn statistiikkaa (Solarwinds 2011b)

NPM sisältää älykkäät verkon hälytykset. Ohjelmisto tarjoaa nopean kuvauksen valvottavista ydinpalveluista ja palvelinsalista ryhmitellen valvottavat laitteet dynaamisesti toisiinsa liittyviksi järjestelmiksi ja laitteiksi. Orion antaa hälytyksiä todellisiin ongelmiin käyttämällä kehittyneitä hälytysominaisuuksia (Solarwinds 2011a.)

Orion etsii verkosta laitteita automaattisesti ajoittain sekä pyytää seuraamaan uusia laitteita sekä esittää verkon topologian kuvallisesti. Topologiaa voi seurata visuaalisesti suorituskykyä mittaavilla reaaliaikaisilla statistiikoilla. (Solarwinds 2011a.)

Muokattavia raportteja on saatavilla erittäin laajalta skaalalta verkon suorituskyvyn kannalta. Orionista on mahdollista ajastaa automaattiset raportit verkon laitteista ja suorituskyvystä valmiiksi PDF-muodossa esimerkiksi yrityksen osakkeenomistajille. (Solarwinds 2011a.)

Solarwinds Network Performance Monitor (Orion NPM) on erittäin skaalautuva, laajennettava ja helppo ottaa käyttöön. Ohjelmiston modulaarinen suunnittelu ja joustava lisensointimalli antaa mahdollisuuden ostaa vain mitä tarvitsee. Orion soveltuu hyvin kasvavalle ja suuren yrityksen tarpeisiin. Ohjelmisto toimii muiden Solarwinds-tuotteiden kanssa laajentamalla hallintaominaisuuksia NetFlow-liikenteen analysointiin, kuten IP SLA (Service Level Agreement) WAN (Wide Area Network) -seurantaan, IP-osoitteiden hallintaan, verkon konfigurointiin, käyttäjien seurantaan sekä sovellusten että palvelimien suorituskykyyn. Orion on käyttökunnossa alle tunnissa ilman kalliita konsultteja. (Solarwinds 2011a.)

# 4 VERKONVALVONTASOVELLUSTEN VERTAILU

Verkonvalvontasovelluksen valinta työssä on valittu vertailun kautta. Vertailukriteerit olivat isossa roolissa, joten valintaan oli otettava vain kaksi varsinaisesti vapaan lähdekoodin sovellusta, Zabbix ja Cacti, koska sovelluksissa oli riittävän kattava ja tarpeeksi yksinkertainen käyttöliittymä. Lisäksi ajatellen yhtiön tulevaisuuden laajenemissuunitelmia oli vertailuun otettava vielä yksi maksullinen sovellus, Orion.

## 4.1 Tuotteistuksen kannalta varteenotettavat vertailukriteerit

Työn tutkimusongelmaksi muodostui LahtiNetwork Oy:n pyynnöstä selvittää, onko mahdollista rakentaa järjestelmä erittäin rajatuilla resursseilla ja mahdollisesti jopa tuotteistaa se. Pienen yrityksen ei ole välttämättä järkevää sijoittaa suuria summia alkuun verkonvalvontaan ja siitä mahdollisesti koostuviin lisensseihin. Vasta kun volyymit ovat riitävän suuret, on järkevää maksaa lisensseistä, sitä ennen turvaudutaan kuitenkin ilmaisiin Open Source -sovelluksiin. Samalla on hyvä ottaa huomioon, että tuotteistamalla voitaisiin palvelusta saada jopa rahallista katetta.

Toinen tärkeä nykyajan seikka on yksinkertaisuus ja helppo käyttöliittymä. Mitä helpommin luettavissa ja käytettävissä järjestelmä on, sen paremman arvon sille voi antaa suhteessa monimutkaiseen ja aikaavievään järjestelmään. Monimutkaisia järjestelmiä ei ole aikaa opetella ja käyttää, saati sitten maksaa asiasta konsultille; on siis muistettava pitää asiat yksinkertaisina ja mahdollisimman helppoina itselle ja mahdolliselle asiakkaalle.

Kolmas tärkeä vertailukriteeri on sovelluksen ominaisuudet ja skaalautuvuus. Mitä laajemmat ominaisuudet järjestelmässä on, sitä parempia palveluita voidaan asiakkaalle tuottaa ja tarvittaessa laajentaa palvelua halutusti.

Neljäs vaadittu kriteeri järjestelmälle oli asennuksen dokumentointi eli asennusohje, jotta asennus olisi mahdollista toteuttaa uudestaan nopeasti ja helposti, mikäli

järjestelmä tuotteistettaisiin. Asennusohjeen olisi oltava niin helppo, että jokainen firman työntekijä voisi asennuksen hätätapauksessa ohjeiden avulla suorittaa ja esimerkiksi toimittaa varajärjestelmäksi mahdolliselle asiakkaalle.

## 4.2 Verkonvalvontasovellusten vertailu

Sovelluksien vertailu oli käytännössä toteutettava vain Cactin ja Zabbixin välillä, koska järjestelmän oli oltava alkajaisiksi maksuton. Orion on vertailussa mukana, koska järjestelmä on entuudestaan tuttu LahtiNetworkin työntekijöiden keskuudessa. Mikäli verkonvalvonta saa menestystä, niin päivitetään järjestelmä maksulliseen Solarwinds Orioniin. Ohjelmisto on loppuun asti viimeistelty ja yksinkertainen. Sovelluksista luotiin vertailutaulukko (taulukko 1), josta selviää oleellisimmat järjestelmien ominaisuudet.

TAULUKKO 1. Vertailutaulukko

| Nimi | Cacti | Zabbix | Orion |
|---|---|---|---|
| **IP SLA raportit (IP Service Level Agreements)** | Kyllä | Kyllä | Kyllä |
| **Looginen käyttäjän määriteltävä ryhmäjako** | Kyllä | Kyllä | Kyllä |
| **Trendit** | Kyllä | Kyllä | Kyllä |
| **Trendien ennustus** | Kyllä | Kyllä | Kyllä |
| **Auto Discsovery eli automaattiset havainnot** | Lisäohjelmalla | Yes | Kyllä |
| **Agentti eli valvova ohjelma UNIX ja WIN32 –järjestelmiin** | Ei | Tuettu | Kyllä |
| **SNMP-protokolla tuki** | Kyllä | Kyllä | Kyllä |
| **Syslog-vastaanotto ja -raportointi** | Kyllä | Kyllä | Kyllä |
| **Lisäohjelmat - järjestelmään lisättäviä lisätoimintoja** | Kyllä | Kyllä | Kyllä |
| **Triggerit / Hälytykset – raja-arvojen ylitykset ja hälytykset** | Kyllä | Kyllä | Kyllä |
| **Selain pohjainen käyttöliittymä** | Täysi kontrolli | Täysi kontrolli | Täysi kontrolli |
| **Hajautettu valvonta – kuormituksen usealle palvelimelle** | Kyllä | Kyllä | Kyllä |
| **Laiteinventaario valvottavista laitteista** | Kyllä | Kyllä | Kyllä |

| | | | |
|---|---|---|---|
| **Tallennusmetodi** | RRDtool, MySQL | Oracle, MySQL, PostgreSQL,IBM DB2, SQLite | SQL |
| **Lisenssi** | GPL | GPL | Maksullinen |
| **Topologiakartat** | Lisäohjelma | Kyllä | Kyllä |
| **Käyttäjäoikeudet eriarvoisille käyttäjille** | Kyllä | Kyllä | Kyllä |
| **IPv6 tuki** | Kyllä | Kyllä | Kyllä |

## 4.3 Yhteenveto

Taulukon perusteella tehtiin suora arvio järjestelmistä. Zabbix sisältää kaikki halutut ominaisuudet, mutta Cactista puuttuu agentit ja suora ominaisuus verkon automaattisille havainnoille (Auto Discovery). Erittäin huomattava seikka vertailussa on, että ilmainen Zabbix sisältää samat vertailun ominaisuudet kuin maksullinen Orion, jonka suurimmat erot Zabbixiin ovat kuitenkin lähinnä ulkonäkö, loppuun asti mietityt ominaisuudet, valmiit scriptit, käyttäjätuki, nopea käyttöönotto ja Windows-pohjaisuus. Orion onkin selvästi niille, jotka haluavat käyttää aikansa muihin töihin kuin verkonvalvontajärjestelmän hienosäätöihin, uusien sääntöjen, scriptien luontiin ja mahdollisten ongelmien ratkaisuihin. Onkin hyvä kysyä, onko järkevää ottaa käyttöön ilmainen sovellus ja tuhlata siihen lukematomia työtunteja vai ottaa vähemmillä työtunneilla ja samalla rahalla huoleton sovellus ja keskittyä muihin töihin. Yksi vertailukriteereistähän oli laitteiston yksinkertaisuus ja helppous. Täysin kriteerit eivät täyty Zabbixin kohdalla, mutta rakennettaessa vapaan lähdekoodin järjestelmää, ei täydellisyyttä voi täysin odottaa. Lähinnä täydellisyyttä on vapaan lähdekoodin järjestelmistä Zabbix-verkonvalvontajärjestelmä.

# 5 ASIAKASTARPEIDEN MÄÄRITTELY JA TUOTTEISTUS

## 5.1 Asiakastarpeiden määrittely

Lähtökohtaisesti asiakas haluaa verkonvalvonnalla varmuuden, että verkko on toimintakuntoinen ja verkon varassa olevat palvelut ovat toiminnallisia. Lisäksi asiakas haluaa tiedon ongelmista heti ja statistiikkaa kapasiteetin riittävyydestä ja päätelaitteista. Valvottavia päätelaitteita asiakkaalla voivat olla esimerkiksi palvelin, pc ja tulostin. Isoilla asiakkailla on taas useita aktiivilaitteita, kuten reitittimiä ja kytkimiä ja luonnollisesti myös päätelaitteita. Kaikista laitteista voidaan myös kerätä tarkempaa statistiikkaa.

Mikäli verkkoon tai päätelaitteeseen sattuisi tulemaan vika, olisi siitä hyvä saada tieto mahdollisimman nopeasti. Verkonvalvonnan avulla saadaan generoitua hälytyksiä, jotka voidaan edelleen lähettää valvontajärjestelmästä sähköpostitse tai tekstiviestinä verkkoa hallinnoiville henkilöille. Hälytykset voidaan priorisoida, jolloin esimerkiksi verkon kriittiset palvelut ovat heti havaittavissa ja mahdolliset verkon kuormituspiikit sekä muut virheilmoitukset tallentuvat tietokantaan ja näkyvät statistiikassa, kuvaajissa ja raporteissa.

Tänä päivänä asiakas voi joutua maksamaan verkon kapasiteetista huomattavia summia, joten turhan kapasiteetin ylläpito ei ole järkevää. Tähän tilanteeseen on hyvä kerätä verkosta statistiikkaa, jotta verkon kapasiteetti voitaisiin optimoida. Mikäli kuormitustasot uhkaavat nousta huippuunsa, on mahdollisesti aika harkita kapasiteetin kasvattamista.

## 5.2 Tarjottavat palvelut

Lähtökohtaisesti LahtiNetwork Oy:n on tarkoitus tarjota verkonvalvonta ja hallintapalveluita asiakkaille kuukausi- tai vuosihintaan. Tarkoitus on tarjota kolmea eri pakettivaihtoehtoa, mutta samalla sisällöllä, vain palvelun laajuudesta riippuen. Lisäpalveluna verkonvalvontaan voidaan myöhemmin lisätä palomuuri ja IDS (Intrusion Detection System).

Verkonvalvonta ja -hallintapalvelu käytännössä käsittää verkon aktiivilaitteiden ja päätelaitteiden valvonnan ja hallinnan. Aktiivilaitteilla tarkoitetaan verkon kytkimiä, reitittimiä ja palomuureja, kun taas päätelaitteilla palvelimet, tulostimet ja pc:t. Verkon aktiivilaitteista valvottaisiin kokonaiskuormitusta ja porttikohtaisia tietoja, kuten tila ja kuormitus. Päätelaitteista valvottaisiin palvelimien palveluita, tulostinten toimintaa sekä mahdollisesti henkilöstön tietokoneita.

## 5.3 Verkonvalvonnan ja -hallinnan tuotteistus ja hinnoittelu

Tuotteistus on suunniteltava siten, että alkuun toteutetaan kustannussyistä verkonvalvontajärjestelmä Open Source -sovelluksilla keskitetysti. Vasta kun tilausvoluumit ovat riittävän suuret ja puhutaan yli 20 laitteen valvonnasta, on aika harkita lisenssitason valvontajärjestelmiä paikallisesti asiakkaan järjestelmäään. Tuotteistusesimerkkinä taulukko 2.

TAULUKKO 2. Tuotteistus

| | 1 – 5 laitetta | 5 – 10 laitetta | 20 – 500 laitetta |
|---|---|---|---|
| **Aktiivilaitteet** | x | x | x |
| **Päätelaitteet** | x | x | x |
| **Verkkotopologia** | - | x | x |

Open Source -järjestelmällä voidaan palvelu hinnoitella entistäkin kilpailukykyisemmin. 1 – 20 laitteen valvonta toteutetaan keskitetysti ja siitä suuremmat valvonnat paikallisesti. Tapauskohtaisesti voidaan toteutustavasta neuvotella erikseen. Tuotteille on määritelty kuukausi- ja vuosihinnat, lisäksi on otettava huomioon palvelun laitteistovaatimukset kustannuksia laskettaessa. Paikanpäällä on suoritettava asennustyöt jokaiseen valvottavaan laitteeseen yksilöllisesti. Lisäksi on luotava VPN-tunneli asiakasverkon ja palveluntarjoajan verkonvalvontajärjestelmän välille. Kaikki työt vaativat aikaa, ja aika on rahaa, joten on määriteltävä valvontajärjestelmän käyttöönotolle järkevä hinnoittelutapa. Vaihtoehtoina voitaneen

pitää vaikeissa tapauksissa tuntivelotteista hinnoittelua ja selkeissä tapauksissa urakkahinnoittelua. Yhteenvetona voitaisiin verkonvalvontapalvelua pitää kehityskelpoisena ideana, josta voitaisiin saada aikanaan jopa saada myytävä tuote. Esimerkkihinnastona taulukko 3.

TAULUKKO 3. Hinnasto

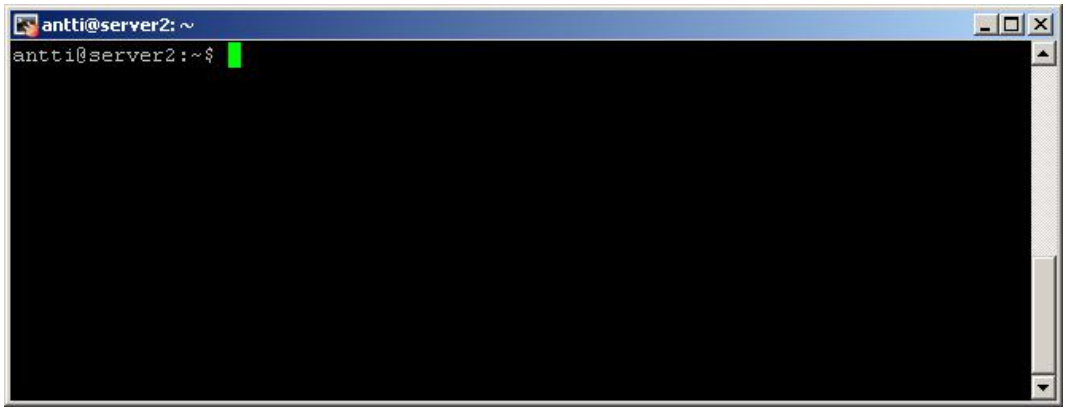
| | **ALV 0%** | **ALV 23%** | **ALV 0%** | **ALV 23%** |
|---|---|---|---|---|
| **1 – 5 laitetta** | 40,0 € / kk | 49,2 € /kk | 400 € / vuosi | 492 € / vuosi |
| **6 – 10 laitetta** | 80, 0 € / kk | 98,4 € / kk | 800 € / vuosi | 984 € / vuosi |
| **11 – 20 laitetta** | 120,0 € / kk | 147,6 € / kk | 1200 € / vuosi | 1476 € / vuosi |
| **20 – X laitetta** | Hinnoittelu tapauskohtaisesti | | | |
| **Suunnittelu ja asennustyöt** | Tuntiveloitus tai urakkahinnoittelu | | | |
| **Muutostyöt** | Tuntiveloitteisena 80 € / h | | | |

# 6 VERKONVALVONTAPALVELUN TOTEUTUS

Zabbix -verkonvalvontapalvelu toteutetaan LahtiNetwork Oy:n tarjoamiin tiloihin, josta järjestelmän on määrä valvoa asiakkaiden lähiverkkoja keskitetysti internetin yli VPN-yhteyksien avulla. Laitteiston rakennusvaiheessa lopullista laitetilaa ei vielä tiedetty, joten rakennettiin mahdollisimman hyvin lopullista tilaa vastaava fyysinen tietoverkkolaboratorio laitteilla, joita oli mahdollista saada käyttöön. Ohjelmistovertailun avulla valittiin toteutettavaksi verkonvalvontajärjestelmäksi palvelulle Zabbix 1.8.5 versio.

Verkonvalvontapalvelun käyttöönoton suunnitelma oli luotava, jotta työlle saatiin järkevä etenemisjärjestys. Käyttöönotto aloitettaisiin verkonhallintaprotokollien käyttöönotolla asiakkaan verkon valvottavissa laitteissa. Tämän jälkeen VPN-yhteys on määriteltävä asiakkaan hallintaverkkoon, minkä jälkeen olisi luotava varayhteys asiakkaan verkkoon esimerkiksi mokkulalla, mikäli asiakkaan internet-yhteys ei toimisi. Kun yhteys olisi muodostettu, niin voitaisiin aloittaa laitteiden automaattinen lisäys järjestelmään Auto Discovery -toiminnolla, joissa on SNMP-protokolla tai agentin määritykset tehty. Kun laitteet näkyvät verkonvalvontajärjestelmässä, on niille määriteltävä sensorit ja niiden raja-arvot, jotka laitteista halutaan valvoa. Raja-arvon ylittyessä verkonvalvontajärjestelmä generoi hälytyksen ja lähettää sen järjestelmän ylläpitäjälle. Lopuksi asiakkaalle luodaan käyttäjätili, josta on rajattu kaikki hallinnallisoikeudet eli mahdollisuus tehdä muokkauksia järjestelmään. Lukuoikeudet voivat esimerkiksi sisältää verkonvalvontajärjestelmän generoimia kuvaajia verkon tilasta, trendeistä ja hälytyksistä. Viimeiseksi olisi tehtävä verkkotopologiankartan määrittely tai päivitys. Topologiakartasta selviäisi asiakkaalle valvottavien laitteiden sijainnit, määritykset ja fyysiset yhteydet muihin verkon laitteisiin.

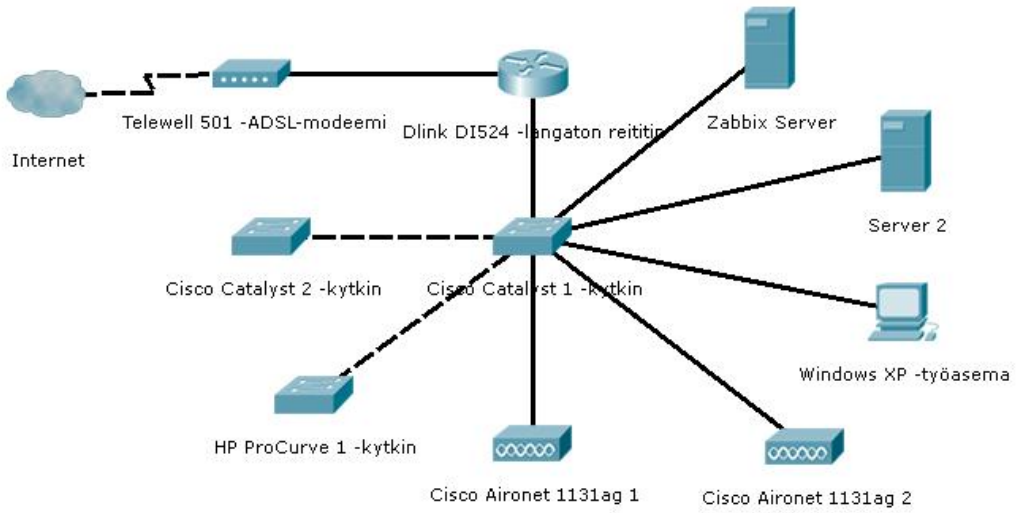
Zabbix 1.8.5 asennettiin vanhalle HP ProLiant DL380 G3 -räkkipalvelimelle Ubuntu Server 11.04 32-bit -käyttöjärjestelmän päälle. Ubuntu Server on Linux-pohjainen avoimeen lähdekoodiin perustuva käyttöjärjestelmä, jossa sovellukset sekä hallinta ovat ohjattavissa terminaalin kautta (kuvio 9). Ubuntu Server oli looginen valinta Zabbixin alustaksi, koska yrityksen henkilöstöllä oli jo ennestään kokemusta kyseisestä järjestelmästä.




KUVIO 9. Terminaalipääte

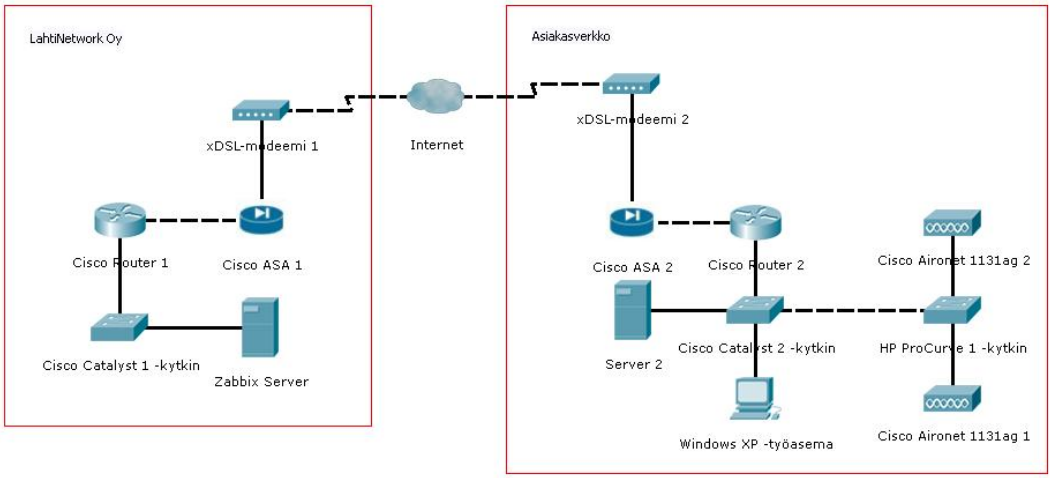
## 6.1 Verkonvalvontapalvelun keskitetty verkkoympäristö

LahtiNetwork Oy:n tietoverkkolaboratorio koostui pienestä lähiverkosta (kuvio 10), jossa oli testilaitteina: D-Link DI-524 langaton reititin, 2 kpl Ciscon Catalyst 2950 24-porttista kytkintä, HP ProCurve Switch 2524 -kytkin, 2 kpl Cisco Aironet 113 -langatonta tukiasemaa, Ubuntu Server 11.04 ja yksi Windows XP -työasema. Työtä tehdessä, ei tietoverkkolaboratorioon saatu tarvittavia laitteita VPN-yhteyden testaamiseen. Kyseisiä laitteita olisivat olleet esimerkiksi 2 kpl Ciscon ASA-palomuureja sekä 2 kpl Ciscon reitittimiä. Kaikki laitteet, joita tietoverkko-laboratoriossa käytettiin, olivat ideaalisia verkon tarpeisiin nähden. Suurin osa yritysverkkojen aktiivilaitteista koostuu kyseisistä vastaavista laitteista.




KUVIO 10. Tietoverkkolaboratorion verkkotopologia

Tarkoitus oli rakentaa tietoverkkolaboratorioon testiverkko, joka olisi simuloinut mahdollisimman hyvin todellisuutta. Kuvio 11 esittää ideaalisen laboratorioverkon verkkotopologian.




KUVIO 11. Ideaalisen laboratorioverkon verkkotopologia

## 6.2 Palvelimen asennus

Zabbix 1.8.5 -ohjelmisto asennettiin Ubuntu Server 11.04 -käyttöjärjestelmälle. Käyttöjärjestelmään oli lisättävä erinäisiä lisäpaketteja Zabbix:n ohjelmiston vaatimuksien vuoksi. Ensimmäinen asennus palvelimelle oli SSH-ohjelmisto(Secure Shell), jonka avulla on mahdollista ottaa palvelimeen etäyhteys. Lisäksi oli asennettava useita muita lisäpaketteja, kuten Apache, MySQL, PHP, SNMP ja fping. Kaikki lisäpakettien asennukset onnistuivat helposti.

Asennusten jälkeen palvelimelle määriteltiin käyttäjätunnus Zabbix ja siirryttiin Zabbix-käyttäjäksi, jolloin kaikki muutokset ja ohjelmiston oikeudet tapahtuvat zabbix-käyttäjän nimissä. MySQL-tietokannalle oli myös määriteltävä tunnus ja salasana, jonka jälkeen voitiin vasta asentaa Zabbix-ohjelmisto, joka sisältää palvelintoiminnot, mysql-tietokantataulukon, webbikäyttöliittymän ja agentin itsensä tarkkailuun. Tämän jälkeen oli tehtävä vielä useita eri määrityksiä palvelimelle, jotta palvelusta saadaan toimiva. Tarkemmat step-by-step-ohjeet palvelimen pystyttämiseen löytyy opinnäytetyön liitteestä 1.

## 6.3 SNMP:n ja Agenttien määritykset verkkolaitteissa

Testiverkon laitteissa otettiin SNMP-agentit käyttöön yksinkertaisesti määrittelemällä agentille haluttu snmp-community-tunnus. Kaikissa valvottavissa laitteissa on oltava yhtenäiset versiot ja SNMP-community-avaimet. Sama koskee myös valvovaa laitetta eli Zabbix-palvelinta. Telewell ADSL -modeemissa ei SNMP-tukea löytynyt ja Windows XP -työasemaan ja Server 2 -palvelimeen oli SNMP-tuki asennettava lisäpakettina. Server 2 -palvelimeen asennettiin myös Zabbixin oma agenttisovellus, joka tarkkaili huomattavasti laajemmin palvelinta kuin SNMP-protokolla.

SNMP-protokolla toimi testilaitteissa moitteettomasti. Zabbix-agenttisovellus toi kattavat valvontamahdollisuudet palvelimelle ja työasemalle. Valmiita raja-arvoja oli valmiiksi oletuksena jopa liikaa, mikä kuormitti verkonvalvontapalvelinta turhankin paljon, joten turhat valvottavat objektit riisuttiin pois ja jätettiin vain halutut. Esimerkkinä turhista valvottavista objekteista voidaan mainita kaikki palvelimien sisäiset palvelut, joita ei vielä tässä vaiheessa haluttu valvoa, kuten sähköpostipalvelin, tietokantapalvelin ja muut sadat objektit. Verkonvalvontajärjestelmän kuormitus keveni huomattavasti poistamalla turhat valvottavat objektit. Tärkein valvottava asia oli, että laittet vastasivat ping-kyselyyn, tämän avulla saatiin riittävä tieto, että laitteet olivat toiminnassa.

## 6.4 VPN-yhteys ja varayhteys valvottavaan verkkoon

VPN-yhteydet oltaisiin luotu käyttämällä Ciscon Asa -palomuuria, koska Cisco on käytetyimpiä valmistajia mutta valitettavasti emme saaneet toista Asaa testijärjestelmään, jotta olisimme voineet todeta VPN-yhteyden toimivuuden. Käytännössä Zabbix-palvelin ei olisi Asan muodostamaa VPN-yhteyttä asiakkaan verkkoon edes huomannut, joten ylimääräisiä määrityksiä ei Zabbix-palvelimeen olisi tarvinnut luoda juuri ollenkaan, paitsi asiakasryhmä ja sille vain asiakkaan valvotut laitteet. Palomuurilla olisi voitu verkot pitää erossa toisistaan ja täten asiakkaat eivät olisi tietoisia toisistaan, mikäli heitä olisi useampia samassa keskitetyssä verkonvalvontajärjestelmässä.

Varayhteys olisi välttämätön, kun kyseessä on verkonvalvontajärjestelmä. Reittejä keskitetylle verkonvalvontajärjestelmälle olisi oltava kaksi asiakkaalta. Kuluttajaystävällisimmäksi vaihtoehdoksi voidaan määritellä asiakkaalle varayhteydeksi mokkula eli langattoman UMTS-laajakaista. Varayhteys olisi yksinkertaisimmillaan vain muodostettu reitittimellä siten, että kun ensisijainen VPN-yhteys katkeaa, ohjaa reititin VPN-yhteyden uudestaan asiakkaan mokkulaan. Järjestelmää ei päästy testaamaan opinnäytetyön puitteissa.

## 6.5 Auto Discovery

Auto Discovery -toiminnolla voidaan hakea halutusta IP-osoiteavaruudesta kaikki laitteet esimerkiksi pelkällä ping-lähetys-vastaus-metodilla, jolloin kaikki ping-kyselyyn vastanneet laitteet päätyvät automaattisesti järjestelmän listalle aiemmin valitusta IP-osoiteavaruudesta. Auto Discovery -toimintoja on erilaisia, Zabbix-järjestelmässä käyttäjä saa itse luoda Auto Discovery toiminnon valitsemillaan laitteen löytömetodeilla.

Tässä opinnäytetyössä käytettiin ping-kyselyä. Auto Discoveryn olisi voinut myös määrittämään etsimään ainoastaan SNMP-protokollaa käyttävät laitteet verkosta tai Zabbixin agenttia käyttävät laitteet. Kyseisellä tavalla saatiin samalla luotua automaattisia laiteryhmiä, jolla voitiin erotella laitteet toisistaan. Esimerkiksi kaikki SNMP-protokollaa käyttävät laitteet määriteltiin verkon aktiivilaitteiksi ja agentteja käyttävät laitteet päätelaitteiksi.

## 6.6 Trigger, Action, sähköpostihälytys

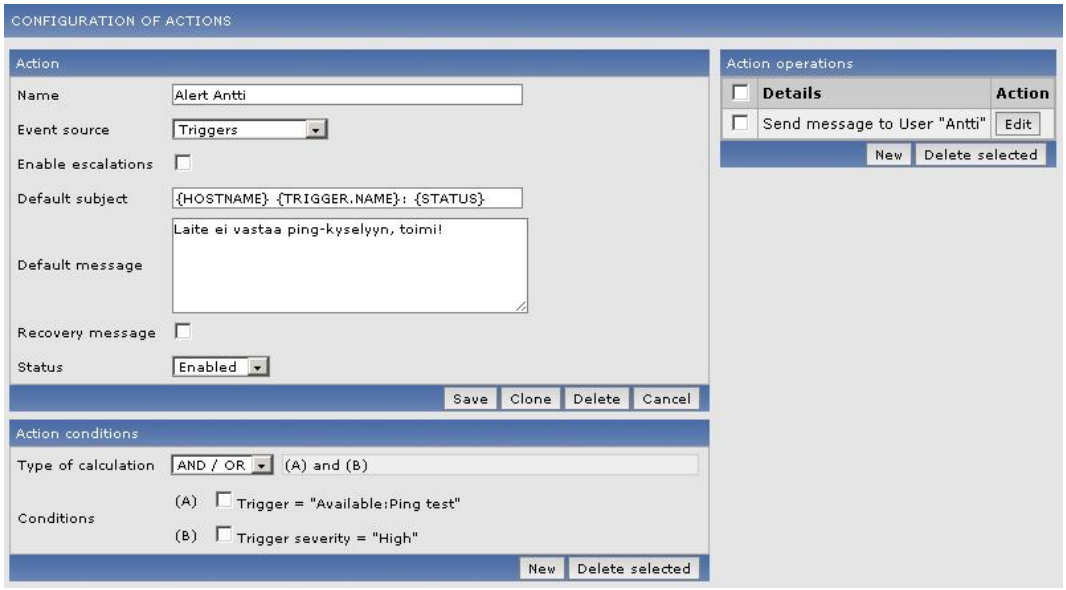
Triggerit ovat avain valvontaan; ne seuraavat laitteiden agenttien informoimaa dataa. Triggerit aktivoituvat, kun laitteilta saatu data on ylittänyt ennalta määritetyn raja-arvon. Zabbix -verkonvalvontasovelluksessa hälyksen teko on kaksivaiheinen prosessi, jossa pitää ensin luoda Trigger ja vasta sitten luoda Action (kuvio

12), joka seuraa Triggerin tilaa ja generoi hälytykset. Sähköpostihälytys luodaan kun laite ei vastaa ping-kyselyyn:

1. Ensin valitaan laiteryhmä tai laitteet, joille ping-kysely tehdään ja annetaan nimeksi Available:
Configuration → Templates → Create Template → Add Groupe / Add Device

2. Luodaan Template:lle Trigger ja annetaan seuraavat arvot:
Configuration → Templates → Triggers → Create Trigger
Name: Ping Test
Expression: {Available:icmpping.last(0)}=0 // Valitaan luettelosta
Severity: High
Comment: Laite ei vastaa ping-kyselyyn

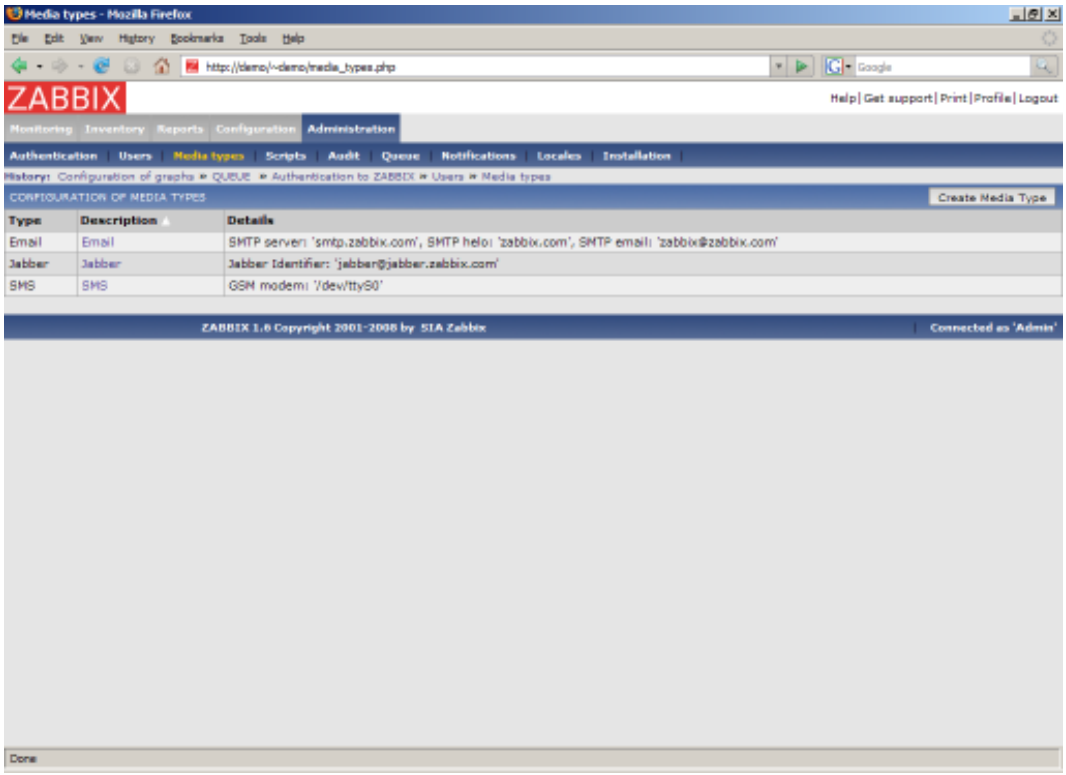
3. Luodaan Action, joka lähettää sähköpostin, kun triggeri aktivoituu:
Configuration → Actions → Create Action




KUVIO 12. Sähköpostihälytys

Vaihtoehtoisesti Action voi myös suorittaa etäkäskyn palvelimelle. Esimerkiksi kun palvelimen MySql-palvelu on jostain syystä kaatunut, niin järjestelmä saa siitä triggerin, jolloin ennalta määritetty Action lähettää palvelimelle /etc/inid.d/MySql restart -etäkäskyn, jolloin MySql-palvelu yrittää käynnistää it-

sensä automaattisesti takaisin ylös. Vastaavilla Action:illa voidaan automatisoida ongelmallisten palveluiden korjauksia ja säästää ylläpidon resursseja. Jotta etäkäskyt toimisivat, on Remote commands määriteltävä käyttöön zabbix_agentd.conf-tiedostoon. Sähköpostihälytykset järjestelmästä puhelimeen toimivat moitteettomasti halutun raja-arvon ylittyessä.




KUVIO 13. Vaihtoehtoiset hälytystavat

Zabbix-verkonvalvontajärjestelmään oli tarkoitus asentaa GSM-modeemi eli mokkula, jolla teksiviestihälytykset olisivat mahdollisia. Palvelin käyttöjärjestelmä ei kuitenkaan tukenut uutta Nokia-merkkistä mokkulaa, joten SMS-viestejä ei työn aikana saatu testattua. Vaihtoehtoisia hälytystapoja (kuvio 13) järjestelmässä on sähköposti, Jabber (pikaviestin) ja tekstiviestit gsm-modeemilla tai scriptin avulla internetpalvelun kautta.

## 6.7 Käyttäjäryhmien luonti

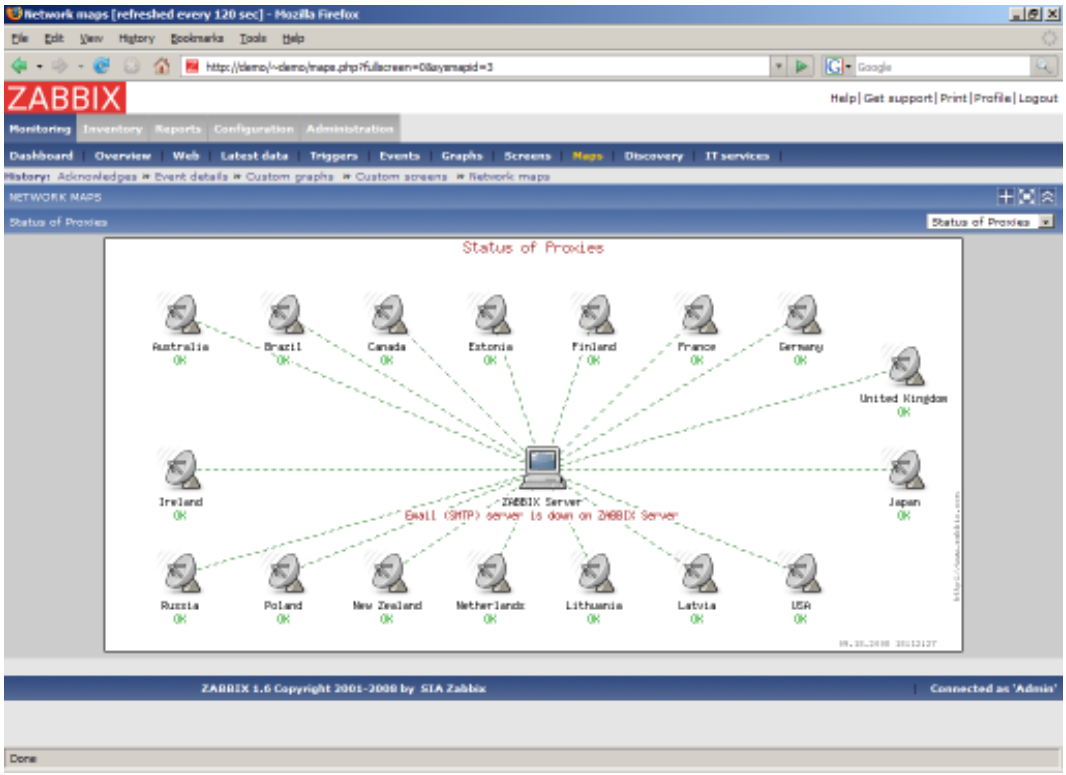
Käyttäjäryhmillä ja käyttäjäoikeuksilla varmistetaan, ettei kukaan osaamaton henkilö voi vahingossa muuttaa palvelimen kriittisiä palveluja siten, ettei palvelu välttämättä enää toimisi siten kuin on tarkoitettu. Käyttäjäryhmiä on hyvä olla

useita. Tärkeää olisi, ettei kirjoitusoikeuksilla koskaan mentäisi lukemaan tietoa, jolloin vältyttäisiin vahingoilta. Palvelimen statistiikoita olisi siis hyvä lukea ainoastaan lukuoikeuksilla. Samalla voidaan estää tiettyjen palveluiden näkyminen kokonaan halutuilta käyttäjiltä, jolloin voidaan esimerkiksi palveluiden näkyvyyttä hyödyntää tuotteistuksen kannalta oleellisesti. Palveluista voidaan siis tehdä maksullisia tietyille käyttäjille.

Koska työ on keskitetty verkonvalvontajärjestelmä, on myös luotava käyttäjäryhmiä, joilla on vain lukuoikeudet tiettyihin ip-avaruuksiin ja palveluihin. Täten voidaan samaa verkonvalvontajärjestelmää hyödyntää useammassa verkossa samanaikaisesti tuotteistettuna palveluna.

## 6.8 Topologia-kartan luonti

Topologia-kartta on tärkeä havainnollistava elementti verkonvalvonnassa. Kartan avulla voidaan nopeasti nähdä laitteiden sidonnaisuudet toisiinsa. Karttoja on järjestelmässä oltava yhtä monta kuin on asiakkaitakin, koska jokaiselle asiakkaalle on oltava omasta verkosta saatavilla oleva topologia-kartta.




KUVIO 14. Esimerkki Topologia-kartta (Zabbix SIA 2011c)

Zabbix-verkonvalvontasovelluksessa topologia-kartta oli luotava täysin manuaalisesti yksin. Kaikki laitteet on lisättävä käsin määrittelemällä ne karttapohjalle ja annettava sidosmääritykset yksi kerrallaan. Tämä on suuritöinen ominaisuus, jota ei ole suositeltavaa käyttää, ellei ole ylimääräistä aikaa. Esimerkkinä Zabbixin topologia-kartta kuviossa 14. Vastaavasti maksullisessa Orion – verkonvalvontasovelluksessa oli automaattinen Topologia-kartta. Ohjelma muodosti kartan kokonaisuudessaan automaattisesti. Vastaava toiminnallisuus olisi hyvä myös Zabbixista.

# 7 YHTEENVETO

Opinnäytetyön tavoitteena oli kehittää LahtiNetwork Oy:lle verkonvalvontajärjestelmä, joka tulisi yhtiön tulevaan omaan konesaliin. Tavoitteena oli selvittää mahdollisimman monipuolinen, edullinen, dokumentoitu ja helppokäyttöinen järjestelmä, joka voitaisiin myöhemmässä vaiheessa jopa tuotteistaa palveluksi osaksi yrityksille tarjottaviin internetliittymiin. Työssä lisäksi perehdyttiin verkonhallintaan ja siihen liittyvään verkonvalvontaan sekä verkonhallinan oleellisimpaan SNMP-protokollaperheeseen. Opinnäytetyössä myös perehdyttiin OSI-malliin, koska tietoliikennejärjestelmät pitkälti perustuvat OSI-malliin.

Zabbix verkonvalvontasovellus osoittautui opinnäytetyön vertailussa parhaaksi vapaan lähdekoodin sovellukseksi ohjelman kattavista ominaisuuksista johtuen. Ohjelmisto oli vertailussa Cactia selvästi kehittyneempi ja yksinkertaisempi käyttää. Lisäksi Cactista puuttui kokonaan Auto Discovery ja agentit, jotka olivat valittavan ohjelmiston vaatimuksia. Samalla vertailtiin myös maksullista Solarwinds Orion -verkonvalvontasovellusta, jotta ilmaisen ja maksullisen verkonvalvontasovelluksen ero tulisi selväksi. Mikäli verkonvalvontapalvelu kasvaisi merkittävästi, olisi LahtiNetwork Oy:n loogisinta siirtyä maksulliseen verkonvalvontapalveluun.

Työn tavoitteet eivät täysin käyneet toteen, mutta toimiva verkonvalvontajärjestelmä tuli kuitenkin onnistuneesti rakennettua. Järjestelmä ei ole vielä käytössä, koska LahtiNetwork Oy:n palvelinsali on vielä rakenteilla. Kuitenkin järjestelmässä toimivat sähköpostihälytykset ja valvottavat laitteet löytyvät jäjestelmästä. Tuotteistuksen kannalta opinnäytetyön avulla saatiin perusajatus, miten verkonvalvontajärjestelmä voitaisiin tuotteistaa palveluksi. Kaiken kaikkiaan opinnäytetyö oli onnistunut projekti, jonka avulla voidaan myöhemmin ottaa suunniteltu järjestelmä käyttöön nopeasti ja helposti.

Tulevaisuudessa järjestelmä tullaan ottamaan käyttöön LahtiNetwork Oy:n palvelinsaliin. Laitesalista löytyy varmennettu kuituyhteys kahdesta suunnasta, upsivarmennettu sähkönsyöttö kahdesta suunnasta, korotettu lattia, hiilidioksidipalosammutusjärjestelmä sekä ympäristöystävällinen ja ekologinen pohjavesijäähdytys. Laitesalin hukkalämpö tullaan käyttämään rakennuksen lämmittämiseen.

Verkonvalvonta on tärkeää verkoissa, koska sen avulla voidaan mitata verkon suorituskykyä ja selvittää pullonkaulat. Kaatuneista tai sammuneista laitteista saadaan hälytys, jolloin yrityksissä ei pääse syntymään pitkiä katkoksia työnteossa. Pidemmät tietoliikennekatkokset isoissa yrityksissä, joissa työnteko on pitkälti internetistä kiinni, saattaisivat tulla erittäinkin kalliiksi, mikäli verkko olisi alhaalla. Verkonvalvonnalla voidaan myös säästää sähköä, koska laitteiston keräämän statistiikan perusteella voidaan sammuttaa laitteita, kun niitä ei tarvita. Ajattelemalla vihreästi säästämme luontoa ja voimme kehittää tietotekniikkaa normaalista poiketen parempaan suuntaan.

LÄHTEET

Hakala, M & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo.

Microsoft TechNet. 2011. Network Management for Microsoft Networks Using SNMP. [viitattu 15.10.2011]. Saatavissa: http://technet.microsoft.com/en-us/library/cc723469.aspx

Network Management Software. 2011. SNMP Tutorial Part 2. [viitattu 20.10.2011]. Saatavissa: http://www.networkmanagementsoftware.com/snmp-tutorial-part-2-rounding-out-the-basics

Puska, M. 2000. Lähiverkkojen tekniikka -Pro Training. Jyväskylä: Gummerus.

RFC1157. 1990. A Simple Network Management Protocol (SNMP). [viitattu 10.10.2011]. Saatavissa: http://www.ietf.org/rfc/rfc1157.txt

RFC1213. 1991. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. [viitattu 15.10.2011]. Saatavissa: http://tools.ietf.org/rfc/rfc1213.txt

RFC2578. 1999. Structure of Management Information Version 2 (SMIv2). [viitattu 23.10.2011]. Saatavissa: http://tools.ietf.org/rfc/rfc2578.txt

RFC2819. 2000. Remote Network Monitoring MIB. [viitattu 26.10.2011]. Saatavissa: http://tools.ietf.org/rfc/rfc2819.txt

SNMP Research International inc. 2011. The SNMP Protocol [viitattu 14.10.2011]. Saatavissa: http://www.snmp.com/protocol/

Solarwinds. 2011a. Product Info. [viitattu 5.10.2011]. Saatavissa: http://www.solarwinds.com/products/network-management/network-performance-monitor.aspx

Solarwinds. 2011b. Network Performance Monitoring. [viitattu 5.10.2011]. Saatavissa: http://www.solarwinds.com/products/orion/network_monitoring_screen.aspx

The Cacti Group. 2011a. What is Cacti. [viitattu 2.11.2011]. Saatavissa: http://www.cacti.net/what_is_cacti.php

The Cacti Group. 2011b. [viitattu 2.11.2011]. Saatavissa: http://www.cacti.net/image.php?image_id=43

Wikipedia 2011a. Simple Network Management Protocol. [viitattu 15.10.2011] Saatavissa: http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Wikipedia 2011b. Management information base. [viitattu 16.10.2011]. Saatavissa: http://en.wikipedia.org/wiki/Management_information_base

Wikipedia 2011c. RMON. [viitattu 20.10.2011]. Saatavissa: http://en.wikipedia.org/wiki/RMON

Wikipedia 2011d. OSI-malli.[viitattu 20.10.2011]. Saatavissa: http://fi.wikipedia.org/wiki/OSI-malli

Zabbix SIA. 2011a. About Zabbix. [viitattu 1.11.2011]. Saatavissa: http://www.zabbix.com/documentation/1.8/manual/about

Zabbix SIA. 2011b. Screenshots. [viitattu 1.11.2011]. Saatavissa: http://www.zabbix.com/screenshots.php

Zabbix SIA. 2011c. Screenshots. [viitattu 10.8.2011]. Saatavissa: http://www.zabbix.com/screenshots.php

LIITTEET

LIITE 1/1. Palvelimen asennusohje

Jotta Zabbix 1.8.5 ohjelmisto voitaisiin asentaa puhtaalle Ubuntu Server 11.04 käyttöjärjestelmälle, on siihen asennettava ensin useita eri ohjelmia. Zabbix:n sivuilla oli hieman huonot step-by-step-ohjeet, mutta hieman tarkemmalla asiaan paneutumisella kokoontui seuraavanlainen asennusohje:

1. Asennetaan ensin SSH, jotta asennukset voidaan tehdä etänä.
**sudo apt-get install openssh-server**

2. Tarkistetaan asennettavat ohjelmat:
**sudo apt-cache showpkg zabbix-server-mysql**

3. Asennetaan tarvittavat ohjelmat (Apache, MySQL, PHP, SNMP, fping jne.).
**sudo apt-get install apache2 php5-mysql libapache2-mod-php5 mysql-server**
**sudo apt-get install build-essential snmp libsnmp-dev snmpd libcurl4-openssl-dev fping**

4. Luodaan admin käyttäjä zabbix ja siirrytään zabbix käyttäjäksi.
**sudo adduser zabbix**
**sudo adduser zabbix admin**
**su zabbix**
**bash**

5. Annetaan salasana MySQL-käyttäjälle root.
**sudo mysqladmin -u root password haluttusalasana**

6. Tarkistetaan mitä osoitetta MySQL kuuntelee.
**sudo netstat -tap | grep mysql**

LIITE 1/2

Mikäli tulostus näyttää seuraavalta:
**tcp 0 0 localhost.localdo:mysql *:* LISTEN 2713/mysqld**
Tarkoittaa se, että MySQL kuuntelee ainoastaan osoitetta localhost.localdomain, silloin tietoturva on kunnossa.

Mutta, mikäli tulostus on seuraavanlainen:
**tcp 0 0 *:mysql *:* LISTEN 2713/mysqld**
On annettava mysql-salasana myös hostname:lle, koska muutoin kuka tahansa voi päästä käsiksi tietokantaan ja muokata dataa.
**mysqladmin -h lahtinetwork.fi -u root password haluttusalasana**

7. Asennetaan Zabbix-server, -tietokanta, -frontend ja -agent.
**sudo apt-get install zabbix-server-mysql zabbix-frontend-php zabbix-agent**

8. Määritetään valvovan zabbix-serverin tiedot:
**sudo nano /etc/zabbix/zabbix_agentd.conf**
Server=localhost → Server=192.168.0.10
Hostname= → Hostname=lahtinetwork.fi
Tallennus
Agentin uudelleen käynnistys
**sudo /etc/init.d/zabbix-agent restart**

9. Määritetään salasana MySQL zabbix –käyttäjälle webbikäyttöliittymään:
**sudo nano /etc/zabbix/dbconfig.php**

$DB_TYPE=’MYSQL’;
$DB_SERVER=’localhost’;
$DB_DATABASE=’zabbix’;
$DB_USER=’zabbix’;
$DB_PASSWORD=’zabbixsqlsalasana’;

10. Testataan webbikäyttöliittymän toimivuus selaimessa
http://lahtinetwork.fi/zabbix tai http://192.168.0.5/zabbix
**Oletuskäyttäjätunnus: Admin**
**Oletussalasana: zabbix**

11. Tarkistetaan logeista, ettei virheitä asennuksen aikana tapahtunut:
**sudo nano /var/log/zabbix-agent/zabbix_agentd.log**
**sudo nano /var/log/zabbix-server/zabbix_server.log**

12. Zabbix configurointi tiedostot löytyvät:
sudo nano /etc/zabbix/apache.conf
sudo nano /etc/zabbix/dbconfig.php
sudo nano /etc/zabbix/zabbix_agentd.conf
sudo nano /etc/zabbix/zabbix_server.conf

13. Tarkistetaan, että fping on asentunut oikein:
sudo nano /etc/zabbix/zabbix_server.conf
Jos fping-komennon oikea sijainti on /bin/, niin se on muutettava.
/sbin/ → /bin/

14. Pakotetaan SSL-tuki käyttöliittymälle

Asennetaan ssl-tukipaketti:
**sudo apt-get install ssl-cert**

Luodaan ssl-kansio:
**sudo mkdir /etc/apache2/ssl**

Kovakoodataan sertifikaatin kesto:
**sudo make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/apache2/ssl/apache.pem**

Asennetaan SSL-moduuli:
**sudo a2enmod ssl**

**sudo /etc/init.d/apache2 force-reload**

Luodaan virtuaalihost ja varmuuskopioidaan vanha:
**sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/ssl**

Muokataan tiedostoa:
**sudo nano -w /etc/apache2/sites-available/ssl**
NameVirtualHost *:443
<virtualhost *:443>
ServerAdmin webmaster@localhost

SSLEngine On
SSLCertificateFile /etc/apache2/ssl/apache.pem

Otetaan SSL virtualhost käyttöön:
**sudo a2ensite ssl**
**sudo /etc/init.d/apache2 reload**

Mikäli haluttaisiin kuitenkin säilyttää portti 80 käyttöliittymälle, on muokattava tiedostoa:
**sudo nano /etc/apache2/sites-available/default**
NameVirtualHost *:80
<virtualhost *:80>